Atmic Networks

CERTIFICATION EXAM SUPPORT

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE

Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.

Stay connected with our support team
for the latest file updates and exam-related information.

www.atmicnetworks.com

Knowledge that moves beyond memorization.

Question: 1

The MAIN benefit of implementing a data loss prevention (DLP) solution is to:

A. enhance the organization's antivirus controls.
B. eliminate the risk of data loss.
C. complement the organization's detective controls.
D. reduce the need for a security awareness program.

Answer: C

Explanation:

A data loss prevention (DLP) solution is a type of detective control that monitors and prevents unauthorized transmission or leakage of sensitive data from the organization. A DLP solution can enhance the organization's antivirus controls by detecting and blocking malicious code that attempts to exfiltrate data, but this is not its main benefit. A DLP solution cannot eliminate the risk of data loss, as there may be other sources of data loss that are not covered by the DLP solution, such as physical theft, accidental deletion, or natural disasters. A DLP solution also does not reduce the need for a security awareness program, as human factors are often the root cause of data loss incidents. A security awareness program can educate and motivate employees to follow security policies and best practices, and to report any suspicious or anomalous activities. Reference = ISACA, CISM Review Manual, 16th Edition, 2020, page 79.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1003.

Question: 2

During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?

A. Post-incident review
B. Eradication
C. Containment
D. Identification

Answer: B

Explanation:

The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying

and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2. The other phases of incident response are:

Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.

Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.

Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.

Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.

Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1. Reference = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2: What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

Question: 3

Which of the following is PRIMARILY determined by asset classification?

A. Insurance coverage required for assets
B. Level of protection required for assets
C. Priority for asset replacement
D. Replacement cost of assets

Answer: B

Explanation:

Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is

proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other criteria such as risk appetite, business impact, availability and market value4. Reference = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

Question: 4

ACISO learns that a third-party service provider did not notify the organization of a data breach that affected the service provider's data center. Which of the following should the CISO do FIRST?

A. Recommend canceling the outsourcing contract.
B. Request an independent review of the provider's data center.
C. Notify affected customers of the data breach.
D. Determine the extent of the impact to the organization.

Answer: D

Explanation:

The CISO should first determine the extent of the impact to the organization by assessing the nature and scope of the data breach, the type and sensitivity of the data involved, the potential harm to the organization and its customers, and the legal and contractual obligations of the organization and the service provider. This will help the CISO to prioritize the appropriate actions and resources to respond to the incident and mitigate the risks. The other options are possible actions that the CISO may take after determining the impact, depending on the circumstances and the outcomes of the investigation. Reference = CISM Review Manual 15th Edition, page 2231; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1030

Question: 5

An information security manager developing an incident response plan MUST ensure it includes:

A. an inventory of critical data.
B. criteria for escalation.
C. a business impact analysis (BIA).
D. critical infrastructure diagrams.

Answer: B

Explanation:

An incident response plan is a set of procedures and guidelines that define the roles and

responsibilities of the incident response team, the steps to follow in the event of an incident, and the communication and escalation protocols to ensure timely and effective resolution of incidents. One of the essential components of an incident response plan is the criteria for escalation, which specify the conditions and thresholds that trigger the escalation of an incident to a higher level of authority or a different function within the organization. The criteria for escalation may depend on factors such as the severity, impact, duration, scope, and complexity of the incident, as well as the availability and capability of the incident response team. The criteria for escalation help to ensure that incidents are handled by the appropriate personnel, that management is kept informed and involved, and that the necessary resources and support are provided to resolve the incident. Reference = https://blog.exigence.io/a-practical-approach-to-incident-management-escalationhttps://www.uc.edu/content/dam/uc/infosec/docs/Guidelines/Information_Security_Incident_Response_Escalation_Guideline.pdf

Question: 6

Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A. Including service level agreements (SLAs) in vendor contracts
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Performing integration testing with vendor systems

Answer: A

Explanation:

The best way to support the incident management process for attacks on an organization's supply chain is to establish communication paths with vendors. This means that the organization and its vendors have clear and agreed-upon channels, methods, and protocols for exchanging information and coordinating actions in the event of an incident that affects the supply chain. Communication paths with vendors can help to identify the source, scope, and impact of the incident, as well as to share best practices, lessons learned, and recovery strategies. Communication paths with vendors can also facilitate the escalation and resolution of the incident, as well as the reporting and documentation of the incident. Communication paths with vendors are part of the incident response plan (IRP), which is a component of the information security program (ISP) 12345.
The other options are not the best ways to support the incident management process for attacks on the organization's supply chain. Including service level agreements (SLAs) in vendor contracts can help to define the expectations and obligations of the parties involved in the supply chain, as well as the penalties for non-compliance. However, SLAs do not necessarily address the specific procedures and requirements for incident management, nor do they ensure effective communication and collaboration among the parties. Requiring security awareness training for vendor staff can help to reduce the likelihood and severity of incidents by enhancing the knowledge and skills of the vendor personnel who handle the organization's data and systems. However, security awareness training does not guarantee that the vendor staff will follow the appropriate incident management processes, nor does it address the communication and coordination issues that may arise during an incident. Performing integration testing with vendor systems can help to ensure the compatibility and

functionality of the systems that are part of the supply chain, as well as to identify and mitigate any vulnerabilities or errors that could lead to incidents. However, integration testing does not cover all the possible scenarios and risks that could affect the supply chain, nor does it provide the necessary communication and response mechanisms for incident management. Reference = 1, 2, 3, 4, 5 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident- management-part-1 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information- security-incident-management-part-1

Question: 7

Which of the following BEST ensures information security governance is aligned with corporate governance?

A. A security steering committee including IT representation

B. A consistent risk management approach
C. An information security risk register
D. Integration of security reporting into corporate reporting

Answer: D

Explanation:

The best way to ensure information security governance is aligned with corporate governance is to integrate security reporting into corporate reporting. This will enable the board and senior management to oversee and monitor the performance and effectiveness of the information security program, as well as the alignment of information security objectives and strategies with business goals and risk appetite. Security reporting should provide relevant, timely, accurate, and actionable information to support decision making and accountability. The other options are important components of information security governance, but they do not ensure alignment with corporate governance by themselves. Reference = CISM Review Manual 15th Edition, page 411; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1027

Question: 8

Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?

A. Perform a risk assessment.
B. Reduce security hardening settings.
C. Inform business management of the risk.
D. Document a security exception.

Answer: A

Explanation:

Security hardening is the process of applying security configuration settings to systems and software to reduce their attack surface and improve their resistance to threats1. Security hardening settings are based on industry standards and best practices, such as the CIS Benchmarks2, which provide recommended security configurations for various software applications, operating systems, and network devices. However, security hardening settings may not always be compatible with the business requirements and objectives of an organization, and may negatively impact the functionality, performance, or usability of the systems and software3. Therefore, before applying any security hardening settings, an information security manager should perform a risk assessment to evaluate the potential benefits and drawbacks of the settings, and to identify and prioritize the risks associated with them. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses. A risk assessment helps the information security manager to balance the security and business needs of the organization, and to communicate the risk level and impact to the relevant stakeholders. A risk assessment should be performed first, before taking any other actions, such as reducing security hardening settings, informing business management of the risk, or documenting a security exception, because it provides the necessary information and justification for making informed and rational decisions. Reference = 1: Basics of the CIS Hardening Guidelines | RSI Security 2: CIS Baseline Hardening and Security Configuration Guide | CalCom 3:

CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 145 : CISM Review Manual 15th Edition, page 146 : CISM Review Manual 15th Edition, page 147

Question: 9

Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?

A. To identify the organization's risk tolerance
B. To improve security processes
C. To align security roles and responsibilities
D. To optimize security risk management

Answer: D

Explanation:

= The most important reason to ensure information security is aligned with the organization's strategy is to optimize security risk management. Information security is not an isolated function, but rather an integral part of the organization's overall objectives, processes, and governance. By aligning information security with the organization's strategy, the information security manager can ensure that security risks are identified, assessed, treated, and monitored in a consistent, effective, and efficient manner1. Alignment also enables the information security manager to communicate the value and benefits of information security to senior management and other stakeholders, and to justify the allocation of resources and investments for security initiatives2. Alignment also helps to establish clear roles and responsibilities for information security across the organization, and to foster a culture of security awareness and accountability3. Therefore, alignment is essential for optimizing security risk management, which is the process of balancing the protection of information

assets with the business objectives and risk appetite of the organization4. Reference = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM_Review_Manual Pages 1-30 - Flip PDF Download | FlipHTML5 3: CISM 2020: Information Security & Business Process Alignment 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.1

Question: 10

Which of the following should be the MOST important consideration when establishing information security policies for an organization?

A. Job descriptions include requirements to read security policies.
B. The policies are updated annually.
C. Senior management supports the policies.
D. The policies are aligned to industry best practices.

Answer: C

Explanation:

The most important consideration when establishing information security policies for an organization is to ensure that senior management supports the policies. Senior management support is essential for the successful implementation and enforcement of information security policies, as it demonstrates the commitment and accountability of the organization's leadership to information security. Senior management support also helps to allocate adequate resources, establish clear roles and responsibilities, and promote a security-aware culture within the organization. Without senior management support, information security policies may not be aligned with the organization's goals and objectives, may not be communicated and disseminated effectively, and may not be followed or enforced consistently.

Job descriptions that include requirements to read security policies are a way of ensuring that employees are aware of their security obligations, but they are not the most important consideration when establishing information security policies. The policies should be relevant and applicable to the employees' roles and functions, and should be reinforced by regular training and awareness programs.

The policies should be updated periodically to reflect the changes in the organization's environment, risks, and requirements, but updating them annually may not be sufficient or necessary. The frequency of updating the policies should depend on the nature and impact of the changes, and should be determined by a defined policy review process.

The policies should be aligned with industry best practices, standards, and frameworks, but this is not the most important consideration when establishing information security policies. The policies should also be customized and tailored to the organization's specific context, needs, and expectations, and should be consistent with the organization's vision, mission, and values. Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, pages 37-38.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1009.

Question: 11

Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

A. Threat management is enhanced.
B. Compliance status is improved.
C. Security metrics are enhanced.
D. Proactive risk management is facilitated.

Answer: D

Explanation:

A vulnerability assessment process is a systematic and proactive approach to identify, analyze and prioritize the vulnerabilities in an information system. It helps to reduce the exposure of the system to potential threats and improve the security posture of the organization. By implementing a vulnerability assessment process, the organization can facilitate proactive risk management, which is the PRIMARY benefit of this process. Proactive risk management is the process of identifying, assessing and mitigating risks before they become incidents or cause significant impact to the organization. Proactive risk management enables the organization to align its security strategy with its business objectives, optimize its security resources and investments, and enhance its

resilience and compliance.

A . Threat management is enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Threat management is the process of identifying, analyzing and responding to the threats that may exploit the vulnerabilities in an information system. Threat management is enhanced by implementing a vulnerability assessment process, as it helps to reduce the attack surface and prioritize the most critical threats. However, threat management is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a reactive rather than proactive approach to risk management.

B . Compliance status is improved. This is a secondary benefit of implementing a vulnerability assessment process. Compliance status is the degree to which an organization adheres to the applicable laws, regulations, standards and policies that govern its information security. Compliance status is improved by implementing a vulnerability assessment process, as it helps to demonstrate the organization's commitment to security best practices and meet the expectations of the stakeholders and regulators. However, compliance status is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a result rather than a driver of risk management.

C . Security metrics are enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Security metrics are the quantitative and qualitative measures that indicate the effectiveness and efficiency of the information security processes and controls. Security metrics are enhanced by implementing a vulnerability assessment process, as it helps to provide objective and reliable data for security monitoring and reporting. However, security metrics are not the PRIMARY benefit of implementing a vulnerability assessment process, as they are a means rather than an end of risk management.

Reference =

CISM Review Manual 15th Edition, pages 1-301

CISM Exam Content Outline2

Risk Assessment for Technical Vulnerabilities3

A Step-By-Step Guide to Vulnerability Assessment4

Question: 12

When properly implemented, secure transmission protocols protect transactions:

A. from eavesdropping.
B. from denial of service (DoS) attacks.
C. on the client desktop.
D. in the server's database.

Answer: A

Explanation:

Secure transmission protocols are network protocols that ensure the integrity and security of data transmitted across network connections. The specific network security protocol used depends on the type of protected data and network connection. Each protocol defines the techniques and procedures required to protect the network data from unauthorized or malicious attempts to read or exfiltrate information1. One of the most common threats to network data is eavesdropping, which is the interception and analysis of network traffic by an unauthorized third party. Eavesdropping can compromise the confidentiality, integrity, and availability of network data, and can lead to data breaches, identity theft, fraud, espionage, and sabotage2. Therefore, secure

transmission protocols protect transactions from eavesdropping by using encryption, authentication, and integrity mechanisms to prevent unauthorized access and modification of network data. Encryption is the process of transforming data into an unreadable format using a secret key, so that only authorized parties can decrypt and access the data. Authentication is the process of verifying the identity and legitimacy of the parties involved in a network communication, using methods such as passwords, certificates, tokens, or biometrics. Integrity is the process of ensuring that the data has not been altered or corrupted during transmission, using methods such as checksums, hashes, or digital signatures3. Some examples of secure transmission protocols are:

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used protocols for securing web, email, and other application layer communications over the Internet. SSL and TLS use symmetric encryption, asymmetric encryption, and digital certificates to establish secure sessions between clients and servers, and to encrypt and authenticate the data exchanged.

Internet Protocol Security (IPsec), which is a protocol and algorithm suite that secures data transferred over public networks like the Internet. IPsec operates at the network layer and provides end-to-end security for IP packets. IPsec uses two main protocols: Authentication Header (AH), which provides data integrity and authentication, and Encapsulating Security Payload (ESP), which provides data confidentiality, integrity, and authentication. IPsec also uses two modes: transport mode, which protects the payload of IP packets, and tunnel mode, which protects the entire IP packet.

Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over insecure networks. SSH uses encryption, authentication, and integrity to protect the data transmitted between a client and a server. SSH also supports port forwarding, which allows secure tunneling of other network services through SSH connections.

Reference = 1: 6 Network Security Protocols You Should Know | Cato Networks 2: Eavesdropping Attacks - an overview | ScienceDirect Topics 3: Network Security Protocols - an overview | ScienceDirect Topics : SSL/TLS (Secure Sockets Layer/Transport Layer Security) - Definition : IPsec - Wikipedia : Secure Shell - Wikipedia

Question: 13

Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?

A. Metrics to drive the information security program
B. Information security policies
C. A defined security organizational structure
D. An information security strategy

Answer: D

Explanation:

An information security strategy is the most important element to have in place as a basis for developing an effective information security program that supports the organization’s business goals. An information security strategy is a high-level plan that defines the vision, mission, objectives, scope, and principles of information security for the organization1. It also aligns the information security program with the organization’s strategy, culture, risk appetite, and governance framework2. An information security strategy provides the direction, guidance, and justification for the information security program, and ensures that the program is consistent,

coherent, and comprehensive3. An information security strategy also helps to prioritize the information security initiatives, allocate the resources, and measure the performance and value of the information security program4.

The other options are not as important as an information security strategy, because they are either derived from or dependent on the strategy. Metrics are used to drive the information security program, but they need to be based on the strategy and aligned with the goals and objectives of the program. Information security policies are the rules and standards that implement the information security strategy and define the expected behavior and responsibilities of the stakeholders. A defined security organizational structure is the way the information security roles and functions are organized and coordinated within the organization, and it should reflect the strategy and the governance model. Reference = 1: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 2: CISM Review Manual 15th Edition, Chapter 1, Section 1.2 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 4: CISM Review Manual 15th Edition, Chapter 1, Section 1.4 : CISM Review Manual 15th Edition, Chapter 1, Section 1.5 : CISM Review Manual 15th Edition, Chapter 1, Section 1.6 : CISM Review Manual 15th Edition, Chapter 1, Section 1.7

Question: 14

Which of the following is the MOST important consideration when establishing an organization's information security governance committee?

A. Members have knowledge of information security controls.
B. Members are business risk owners.
C. Members are rotated periodically.
D. Members represent functions across the organization.

Answer: D

Explanation:

= The most important consideration when establishing an organization’s information security governance committee is to ensure that members represent functions across the organization. This is because the information security governance committee is responsible for setting the direction, scope, and objectives of the information security program, and for ensuring that the program aligns with the organization’s business goals and strategies. By having members from different functions, such as finance, human resources, operations, legal, and IT, the committee can ensure that the information security program considers the needs, expectations, and perspectives of various stakeholders, and that the program supports the organization’s mission, vision, and values. Having a diverse and representative committee also helps to foster a culture of security awareness and accountability throughout the organization, and to promote collaboration and communication among different functions.

Members having knowledge of information security controls, members being business risk owners, and members being rotated periodically are all desirable characteristics of an information security governance committee, but they are not the most important consideration. Members having knowledge of information security controls can help the committee to understand the technical aspects of information security and to evaluate the effectiveness and efficiency of the information security program. However, having technical knowledge is not sufficient to ensure that the information security program is aligned with the organization’s business goals and strategies, and that the program considers the needs and expectations of various stakeholders. Members being business risk owners can help the committee to identify and prioritize the information security risks that affect the organization’s business objectives, and to allocate appropriate

resources and responsibilities for managing those risks. However, being a business risk owner does not necessarily imply that the member has a comprehensive and balanced view of the organization's information security needs and expectations, and that the member can represent the interests and perspectives of various functions. Members being rotated periodically can help the committee to maintain its independence and objectivity, and to avoid conflicts of interest or complacency. However, rotating members too frequently can also reduce the continuity and consistency of the information security program, and can affect the committee's ability to monitor and evaluate the performance and progress of the information security program.

Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, pages 36-37.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1014.

Question: 15

An information security manager learns that a risk owner has approved exceptions to replace key controls with weaker compensating controls to improve process efficiency. Which of the following should be the GREATEST concern?

A. Risk levels may be elevated beyond acceptable limits.
B. Security audits may report more high-risk findings.
C. The compensating controls may not be cost efficient.
D. Noncompliance with industry best practices may result.

Answer: A

Explanation:

Replacing key controls with weaker compensating controls may introduce new vulnerabilities or increase the likelihood or impact of existing threats, thus raising the risk levels beyond the acceptable limits defined by the risk appetite and tolerance of the organization. This may expose the organization to unacceptable losses or damages, such as financial, reputational, legal, or operational. Therefore, the information security manager should be most concerned about the potential elevation of risk levels and ensure that the risk owner is aware of the consequences and accountable for the decision.

Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, page 941.

Question: 16

Which of the following BEST indicates that information assets are classified accurately?

A. Appropriate prioritization of information risk treatment
B. Increased compliance with information security policy
C. Appropriate assignment of information asset owners
D. An accurate and complete information asset catalog

Answer: A

Explanation:

The best indicator that information assets are classified accurately is appropriate prioritization of information risk treatment. Information asset classification is the process of assigning a level of sensitivity or criticality to information assets based on their value, impact, and legal or regulatory requirements. The purpose of information asset classification is to facilitate the identification and protection of information assets according to their importance and risk exposure. Therefore, if information assets are classified accurately, the organization can prioritize the information risk treatment activities and allocate the resources accordingly. The other options are not direct indicators of information asset classification accuracy, although they may be influenced by it. Reference = CISM Review Manual 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1031

Question: 17

Which of the following is MOST important to include in a post-incident review following a data breach?

A. An evaluation of the effectiveness of the information security strategy
B. Evaluations of the adequacy of existing controls
C. Documentation of regulatory reporting requirements
D. A review of the forensics chain of custom

Answer: B

Explanation:

= A post-incident review is a process of analyzing and learning from a security incident, such as a data breach, to improve the security posture and resilience of an organization. A post-incident review should include the following elements12:

A clear and accurate description of the incident, including its scope, impact, timeline, root cause, and contributing factors.

A detailed assessment of the effectiveness and efficiency of the incident response process, including the roles and responsibilities, communication channels, coordination mechanisms, escalation procedures, tools and resources, documentation, and reporting.

An evaluation of the adequacy of existing controls, such as policies, standards, procedures, technical measures, awareness, and training, to prevent, detect, and mitigate similar incidents in the future. A list of actionable recommendations and improvement plans, based on the lessons learned and best practices, to address the identified gaps and weaknesses in the security strategy, governance, risk management, and incident management.

A follow-up and monitoring mechanism to ensure the implementation and verification of the recommendations and improvement plans.

The most important element to include in a post-incident review following a data breach is the evaluation of the adequacy of existing controls, because it directly relates to the security objectives and requirements of the organization, and provides the basis for enhancing the security posture and resilience of the organization. Evaluating the existing controls helps to identify the vulnerabilities and risks that led to the data breach, and to determine the appropriate corrective and preventive actions to reduce the likelihood and impact of similar

incidents in the future. Evaluating the existing controls also helps to align the security strategy and governance with the business goals and objectives, and to ensure the compliance with legal, regulatory, and contractual obligations.

The other elements, such as an evaluation of the effectiveness of the information security strategy, documentation of regulatory reporting requirements, and a review of the forensics chain of custody, are also important, but not as important as the evaluation of the existing controls. An evaluation of the effectiveness of the information security strategy is a broader and more strategic activity that may not be directly relevant to the specific incident, and may require more time and resources to conduct. Documentation of regulatory reporting requirements is a necessary and mandatory task, but it does not provide much insight or value for improving the security posture and resilience of the organization. A review of the forensics chain of custody is a technical and procedural activity that ensures the integrity and admissibility of the digital evidence collected during the incident investigation, but it does not address the root cause or the mitigation of the incident.

Reference = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM Review Manual 15th Edition, page 147

Question: 18

Which of the following should be the PRIMARY area of focus when mitigating security risks associated with emerging technologies?

A. Compatibility with legacy systems
B. Application of corporate hardening standards
C. Integration with existing access controls
D. Unknown vulnerabilities

Answer: D

Explanation:

= The primary area of focus when mitigating security risks associated with emerging technologies is unknown vulnerabilities. Emerging technologies are new and complex, and often involve multiple parties, interdependencies, and uncertainties. Therefore, they may have unknown vulnerabilities that could expose the organization to threats that are difficult to predict, detect, or prevent1. Unknown vulnerabilities could also result from the lack of experience, knowledge, or best practices in implementing, operating, or securing emerging technologies2. Unknown vulnerabilities could lead to serious consequences, such as data breaches, system failures, reputational damage, legal liabilities, or regulatory sanctions3. Therefore, it is important to focus on identifying, assessing, and addressing unknown vulnerabilities when mitigating security risks associated with emerging technologies.

The other options are not as important as unknown vulnerabilities, because they are either more predictable, manageable, or specific. Compatibility with legacy systems is a technical issue that could affect the performance, functionality, or reliability of emerging technologies, but it is not a security risk per se. It could be resolved by testing, upgrading, or replacing legacy systems4. Application of corporate hardening standards is a security measure that could reduce the attack surface and improve the resilience of emerging technologies, but it is not a sufficient or comprehensive solution. It could be limited by the availability, applicability, or effectiveness of the standards. Integration with existing access controls is a security requirement that could prevent unauthorized or inappropriate access to emerging technologies, but it is not a guarantee of security. It

could be challenged by the complexity, diversity, or dynamism of the access scenarios. Reference = 1: Performing Risk Assessments of Emerging Technologies - ISACA 2: Assessing the Risk of Emerging Technology - ISACA 3: Factors Influencing Public Risk Perception of Emerging Technologies: A … 4: CISM Review Manual 15th Edition, Chapter 3, Section 3.3 : CISM Review Manual 15th Edition, Chapter 3, Section 3.4 : CISM Review Manual 15th Edition, Chapter 3, Section 3.5

Question: 19

Which of the following would be the MOST effective way to present quarterly reports to the board on the status of the information security program?

A. A capability and maturity assessment
B. Detailed analysis of security program KPIs
C. An information security dashboard
D. An information security risk register

Answer: C

Explanation:

An information security dashboard is the most effective way to present quarterly reports to the board on the status of the information security program, because it provides a concise, visual, and high-level overview of the key performance indicators (KPIs), metrics, and trends of the information security program. An information security dashboard can help the board to quickly and easily understand the current state, progress, and performance of the information security program, and to identify any gaps, issues, or areas of improvement. An information security dashboard can also help the board to align the information security program with the organization's business goals and strategies, and to support the decision-making and oversight functions of the board.

A capability and maturity assessment is a way of measuring the effectiveness and efficiency of the information security program, and of identifying the strengths and weaknesses of the program. However, a capability and maturity assessment is not the most effective way to present quarterly reports to the board, because it may not provide a clear and timely picture of the status of the information security program, and it may not reflect the changes and dynamics of the information security environment. A capability and maturity assessment is more suitable for periodic or annual reviews, rather than quarterly reports.

A detailed analysis of security program KPIs is a way of evaluating the performance and progress of the information security program, and of determining the extent to which the program meets the predefined objectives and targets. However, a detailed analysis of security program KPIs is not the most effective way to present quarterly reports to the board, because it may be too technical, complex, or lengthy for the board to comprehend and appreciate. A detailed analysis of security program KPIs is more suitable for operational or tactical level reporting, rather than strategic level reporting.

An information security risk register is a tool for recording and tracking the information security risks that affect the organization, and for documenting the risk assessment, treatment, and monitoring activities. However, an information security risk register is not the most effective way to present quarterly reports to the board, because it may not provide a comprehensive and balanced view of the information security program, and it may not highlight the achievements and benefits of the program. An information security risk register is more suitable for risk management or audit purposes, rather than performance reporting.

Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, pages 47-48, 59-60, 63-64, 67-68.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1019.

An information security dashboard is an effective way to present quarterly reports to the board on the status of the information security program. It allows the board to quickly view key metrics and trends at a glance and to drill down into more detailed information as needed. The dashboard should include metrics such as total incidents, patching compliance, vulnerability scanning results, and more. It should also include high-level overviews of the security program and its components, such as the security policy, security architecture, and security controls.

Question: 20

Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?

A. Cost of the attack to the organization
B. Location of the attacker
C. Method of operation used by the attacker
D. Details from intrusion detection system (IDS) logs

Answer: C

Explanation:

= The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker's motives, skills, and resources, which can help improve the organization's threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. Reference = CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

Question: 21

Which of the following is the MOST important criterion when deciding whether to accept residual risk?

A. Cost of replacing the asset
B. Cost of additional mitigation
C. Annual loss expectancy (ALE)
D. Annual rate of occurrence

Answer: C

Explanation:

= Annual loss expectancy (ALE) is the most important criterion when deciding whether to accept residual risk, because it represents the expected monetary loss for an asset due to a risk over a one- year period. ALE is calculated by multiplying the annual rate of occurrence (ARO) of a risk event by the single loss expectancy (SLE) of the asset. ARO is the estimated frequency of a risk event occurring

within a one-year period, and SLE is the estimated cost of a single occurrence of a risk event. ALE helps to compare the cost and benefit of different risk responses, such as avoidance, mitigation, transfer, or acceptance. Risk acceptance is appropriate when the ALE is lower than the cost of other risk responses, or when the risk is unavoidable or acceptable within the organization's risk appetite and tolerance. ALE also helps to prioritize the risks that need more attention and resources.
Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 22, page 242

Question: 22

An organization is planning to outsource the execution of its disaster recovery activities. Which of the following would be MOST important to include in the outsourcing agreement?

A. Definition of when a disaster should be declared
B. Requirements for regularly testing backups
C. Recovery time objectives (RTOs)
D. The disaster recovery communication plan

Answer: C

Explanation:

The most important thing to include in the outsourcing agreement for disaster recovery activities is the recovery time objectives (RTOs). RTOs are the maximum acceptable time frames within which the critical business processes and information systems must be restored after a disaster or disruption. RTOs are based on the business impact analysis (BIA) and the risk assessment, and they reflect the business continuity requirements and expectations of the organization. By including the RTOs in the outsourcing agreement, the organization can ensure that the service provider is aware of and committed to meeting the agreed service levels and minimizing the downtime and losses in the event of a disaster. The other options are not as important as the RTOs, although they may be relevant and useful to include in the outsourcing agreement depending on the scope and nature of the disaster recovery services. Reference = CISM Review Manual 15th Edition, page 2471; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1033

Question: 23

An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?

A. Determine security controls for the new service.
B. Establish a compliance program,
C. Perform a gap analysis against the current state
D. Hire new resources to support the service.

Answer: C

Explanation:

A gap analysis is a process of comparing the current state of an organization's security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2: It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.

It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.

It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.

It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.

It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.

The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance, which can be derived from the gap analysis. Reference = 1: What is a Gap Analysis? | Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:

1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.infosecinstitute.com+2 more

Question: 24

Which of the following is MOST helpful in determining an organization's current capacity to mitigate risks?

A. Capability maturity model
B. Vulnerability assessment
C. IT security risk and exposure
D. Business impact analysis (BIA)

Answer: A

Explanation:

A capability maturity model (CMM) is a framework that helps organizations assess and improve their processes and capabilities in various domains, such as software development, project management, information security, and others1. A CMM defines a set of levels or stages that represent the degree of maturity or effectiveness of an organization's processes and capabilities in a specific domain. Each level has a set of criteria or characteristics that an organization must meet to achieve that level of maturity. A CMM also provides guidance and best practices on how to progress from one level to another, and how to measure and monitor the performance and improvement of the processes and capabilities2.

A CMM is most helpful in determining an organization's current capacity to mitigate risks, because it provides a systematic and objective way to evaluate the strengths and weaknesses of the organization's processes and capabilities related to risk management. A CMM can help an organization identify the gaps and opportunities for improvement in its risk management practices, and prioritize the actions and resources needed to address them. A CMM can also help an organization benchmark its risk management maturity against industry standards or best practices, and demonstrate its compliance with regulatory or contractual requirements3.

The other options are not as helpful as a CMM in determining an organization's current capacity to mitigate risks, because they are either more specific, limited, or dependent on a CMM. A vulnerability assessment is a process of identifying and analyzing the vulnerabilities in an organization's systems, networks, or applications, and their potential impact on the organization's assets, operations, or reputation. A vulnerability assessment can help an organization identify the sources and levels of risk, but it does not provide a comprehensive or holistic view of the organization's risk management maturity or effectiveness4. IT security risk and exposure is a measure of the likelihood and impact of a security breach or incident on an organization's IT assets, operations, or reputation. IT security risk and exposure can help an organization quantify and communicate the level of risk, but it does not provide a framework or guidance on how to improve the organization's risk management processes or capabilities5. A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of a disruption or disaster on an organization's critical business functions, processes, or resources. A BIA can help an organization determine the priorities and requirements for business continuity and disaster recovery, but it does not provide a method or standard for assessing or enhancing the organization's risk management maturity or effectiveness. Reference = 1: CMMI Institute - What is CMMI? - Capability Maturity Model Integration 2: Capability Maturity Model and Risk Register Integration: The Right … 3: Performing Risk Assessments of Emerging Technologies - ISACA 4: CISM Review Manual 15th Edition, Chapter 4, Section 4.2 5: CISM Review Manual 15th Edition, Chapter 4, Section 4.3 : CISM Review Manual 15th Edition, Chapter 4, Section 4.4

Question: 25

An organization is close to going live with the implementation of a cloud-based application.

Independent penetration test results have been received that show a high-rated vulnerability. Which of the following would be the BEST way to proceed?

A. Implement the application and request the cloud service provider to fix the vulnerability.

B. Assess whether the vulnerability is within the organization's risk tolerance levels.

C. Commission further penetration tests to validate initial test results,
D. Postpone the implementation until the vulnerability has been fixed.

Answer: B

Explanation:

The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization's risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.

Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.

Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information. The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project.

Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact and opportunity cost of postponing the implementation, as it may affect the organization's reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk-averse approach, as it may hinder the organization's innovation and competitiveness. Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1025.

Question: 26

Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

A. Effective security eliminates risk to the business.
B. Adopt a recognized framework with metrics.
C. Security is a business product and not a process.

D. Security supports and protects the business.

Answer: D

Explanation:

The message that security supports and protects the business is the most effective in obtaining senior management's commitment to information security management. This message emphasizes the value and benefits of security for the organization's strategic goals, mission, and vision. It also aligns security with the business needs and expectations, and demonstrates how security can enable and facilitate the business processes and functions. The other messages are not as effective because they either overstate the role of security (A), focus on technical aspects rather than business outcomes (B), or confuse the nature and purpose of security ©. Reference = CISM Review Manual 2022, page 23; CISM Item Development Guide 2022, page 9; CISM Information Security Governance Certified Practice Exam - CherCherTech

Question: 27

Who is BEST suited to determine how the information in a database should be classified?

A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner

Answer: D

Explanation:

= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements. Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them. Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331

Question: 28

In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:

A. evaluate results of the most recent incident response test.
B. review the number of reported security incidents.
C. ensure established security metrics are reported.
D. assess progress of risk mitigation efforts.

Answer: D

Explanation:

According to the CISM Review Manual, an organization's security posture is the overall condition of its information security, which is determined by the effectiveness of its security program and the alignment of its security objectives with its business goals. To understand the security posture, the senior leadership needs to have a holistic view of the security risks and the actions taken to address them. Therefore, assessing the progress of risk mitigation efforts is the most important activity for the senior leadership, as it provides them with the information on how well the security program is performing and whether it is meeting the expected outcomes. Evaluating the results of the most recent incident response test, reviewing the number of reported security incidents, and ensuring established security metrics are reported are all useful activities for the senior leadership, but they are not sufficient to understand the security posture. They only provide partial or isolated information on the security performance, which may not reflect the overall security condition or the alignment with the business objectives. Reference = CISM Review Manual, 16th Edition, Chapter 1, Information Security Governance, pages 28-29.

Question: 29

Which of the following provides an information security manager with the MOST accurate indication of the organization's ability to respond to a cyber attack?

A. Walk-through of the incident response plan
B. Black box penetration test
C. Simulated phishing exercise
D. Red team exercise

Answer: D

Explanation:

A red team exercise is a simulated cyber attack conducted by a group of ethical hackers or security experts (the red team) against an organization's network, systems, and staff (the blue team) to test the organization's ability to detect, respond, and recover from a real cyber attack. A red team exercise provides an information security manager with the most accurate indication of the organization's ability to respond to a cyber attack, because it mimics the tactics, techniques, and

procedures of real threat actors, and challenges the organization's security posture, incident response plan, and security awareness in a realistic and adversarial scenario12. A red team exercise can measure the following aspects of the organization's cyber attack response capability3: The effectiveness and efficiency of the security controls and processes in preventing, detecting, and mitigating cyber attacks

The readiness and performance of the incident response team and other stakeholders in following the incident response plan and procedures

The communication and coordination among the internal and external parties involved in the incident response process

The resilience and recovery of the critical assets and functions affected by the cyber attack The lessons learned and improvement opportunities identified from the cyber attack simulation The other options, such as a walk-

through of the incident response plan, a black box penetration test, or a simulated phishing exercise, are not as accurate as a red team exercise in indicating the organization's ability to respond to a cyber attack, because they have the following limitations4 : A walk-through of the incident response plan is a theoretical and hypothetical exercise that involves reviewing and discussing the incident response plan and procedures with the relevant stakeholders, without actually testing them in a live environment. A walk-through can help to familiarize the participants with the incident response roles and responsibilities, and to identify any gaps or inconsistencies in the plan, but it cannot measure the actual performance and effectiveness of the incident response process under a real cyber attack scenario.

A black box penetration test is a technical and targeted exercise that involves testing the security of a specific system or application, without any prior knowledge or access to its internal details or configuration. A black box penetration test can help to identify the vulnerabilities and weaknesses of the system or application, and to simulate the perspective and behavior of an external attacker, but it cannot test the security of the entire network or organization, or the response of the incident response team and other stakeholders to a cyber attack.

A simulated phishing exercise is a social engineering and awareness exercise that involves sending fake emails or messages to the organization's staff, to test their ability to recognize and report phishing attempts. A simulated phishing exercise can help to measure the level of security awareness and training of the staff, and to simulate one of the most common cyber attack vectors, but it cannot test the security of the network or systems, or the response of the incident response team and other stakeholders to a cyber attack.

Reference = 1: What is a Red Team Exercise? | Redscan 2: Red Team vs Blue Team: How They Differ and Why You Need Both | CISA 3: Red Team Exercises: What They Are and How to Run Them | Rapid7 4: What is a Walkthrough Test? | Definition and Examples | ISACA : Penetration Testing Types: Black Box, White Box, and Gray Box | CISA

Question: 30

Which of the following processes BEST supports the evaluation of incident response effectiveness?

A. Root cause analysis
B. Post-incident review
C. Chain of custody
D. Incident logging

Answer: B

Explanation:

A post-incident review (PIR) is the process of evaluating the effectiveness of the incident response after the incident has been resolved. A PIR aims to identify the strengths and weaknesses of the response process, the root causes and impacts of the incident, the lessons learned and best practices, and the recommendations and action plans for improvement1. A PIR can help an organization enhance its incident response capabilities, reduce the likelihood and severity of future incidents, and increase its resilience and maturity2.

A PIR is the best process to support the evaluation of incident response effectiveness, because it provides a systematic and comprehensive way to assess the performance and outcomes of the response process, and to identify and implement the necessary changes and improvements. A PIR involves collecting and analyzing relevant data and feedback from various sources, such as incident logs, reports, evidence, metrics, surveys, interviews, and observations. A PIR also involves comparing the actual response with the expected or planned response, and measuring the achievement of the response objectives and the satisfaction of the stakeholders3.

A PIR also involves documenting and communicating the findings, conclusions, and recommendations of the evaluation, and ensuring that they are followed up and implemented.
The other options are not as good as a PIR in supporting the evaluation of incident response effectiveness, because they are either more specific, limited, or dependent on a PIR. A root cause analysis (RCA) is a technique to identify the underlying factors or reasons that caused the incident, and to prevent or mitigate their recurrence. An RCA can help an organization understand the nature and origin of the incident, and to address the problem at its source, rather than its symptoms. However, an RCA is not sufficient to evaluate the effectiveness of the response process, because it does not cover other aspects, such as the response performance, outcomes, impacts, lessons, and best practices. An RCA is usually a part of a PIR, rather than a separate process. A chain of custody (CoC) is a process of maintaining and documenting the integrity and security of the evidence collected during the incident response. A CoC can help an organization ensure that the evidence is reliable, authentic, and admissible in legal or regulatory proceedings. However, a CoC is not a process to evaluate the effectiveness of the response process, but rather a requirement or a standard to follow during the response process. A CoC does not provide any feedback or analysis on the response performance, outcomes, impacts, lessons, or best practices. An incident logging is a process of recording and tracking the details and activities of the incident response. An incident logging can help an organization monitor and manage the response process, and to provide an audit trail and a source of information for the evaluation. However, an incident logging is not a process to evaluate the effectiveness of the response process, but rather an input or a tool for the evaluation. An incident logging does not provide any assessment or measurement on the response performance, outcomes, impacts, lessons, or best practices.
Reference = 1: CISM Review Manual 15th Edition, Chapter 5, Section 5.5 2: Post-Incident Review: A Guide to Effective Incident Response 3: PostIncident Review: A Guide to Effective Incident Response : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.4 : CISM Review Manual 15th Edition, Chapter 5, Section 5.3

Question: 31

When deciding to move to a cloud-based model, the FIRST consideration should be:

A. storage in a shared environment.

B. availability of the data.
C. data classification.
D. physical location of the data.

Answer: C

Explanation:

The first consideration when deciding to move to a cloud-based model should be data classification, because it helps the organization to identify the sensitivity, value, and criticality of the data that will be stored, processed, or transmitted in the cloud. Data classification can help the organization to determine the appropriate level of protection, encryption, and access control for the data, and to comply with the relevant legal, regulatory, and contractual requirements. Data classification can also help the organization to evaluate the suitability, compatibility, and trustworthiness of the cloud service provider and the cloud service model, and to negotiate the terms and conditions of the cloud service contract.
Storage in a shared environment, availability of the data, and physical location of the data are all important considerations when deciding to move to a cloud-based model, but they are not the first consideration. Storage

in a shared environment can affect the security, privacy, and integrity of the data, as the data may be co-located with other customers' data, and may be subject to unauthorized access, modification, or deletion. Availability of the data can affect the reliability, performance, and continuity of the data, as the data may be inaccessible, corrupted, or lost due to network failures, service outages, or disasters. Physical location of the data can affect the compliance, sovereignty, and jurisdiction of the data, as the data may be stored or transferred across different countries or regions, and may be subject to different laws, regulations, or policies. However, these considerations depend on the data classification, as different types of data may have different levels of risk, impact, and expectation in the cloud environment. Reference = ISACA, CISM Review Manual, 16th Edition, 2020, pages 95-96, 99-100, 103-104, 107-108. ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1031.

Question: 32

Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?

A. Increase the frequency of system backups.
B. Review the mitigating security controls.
C. Notify staff members of the threat.
D. Assess the risk to the organization.

Answer: D

Explanation:

The best course of action for an information security manager when a threat intelligence report indicates a large number of ransomware attacks targeting the industry is to assess the risk to the organization. This means evaluating the likelihood and impact of a potential ransomware attack on the organization's assets, operations, and reputation, based on the current threat landscape, the organization's security posture, and the effectiveness of the existing security controls. A risk assessment can help the information security manager prioritize the most critical assets and processes, identify the gaps and weaknesses in the security architecture, and determine the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance. A risk assessment can also provide a business case for requesting additional resources or support from senior management to improve the organization's security resilience and readiness. The other options are not the best course of action because they are either too reactive or too narrow in scope. Increasing the frequency of system backups (A) is a good practice to ensure data availability and recovery in case of a ransomware attack, but it does not address the prevention or detection of the attack, nor does it consider the potential data breach or extortion that may accompany the attack. Reviewing the mitigating security controls (B) is a part of the risk assessment process, but it is not sufficient by itself. The information security manager should also consider the threat sources, the vulnerabilities, the impact, and the risk appetite of the organization. Notifying staff members of the threat © is a useful awareness and education measure, but it should be done after the risk assessment and in conjunction with other security policies and procedures. Staff members should be informed of the potential risks, the indicators of compromise, the reporting mechanisms, and the best practices to avoid or respond to a ransomware attack. Reference = CISM Review Manual 2022, pages 77-78, 81-82, 316; CISM Item Development Guide 2022, page 9; #StopRansomware Guide | CISA; [The Human Consequences of Ransomware Attacks - ISACA]; [Ransomware Response, Safeguards and Countermeasures - ISACA]

Question: 33

An organization is going through a digital transformation process, which places the IT organization in an unfamiliar risk landscape. The information security manager has been tasked with leading the IT risk management process. Which of the following should be given the HIGHEST priority?

A. Identification of risk
B. Analysis of control gaps
C. Design of key risk indicators (KRIs)
D. Selection of risk treatment options

Answer: A

Explanation:

= Identification of risk is the first and most important step in the IT risk management process, especially when the organization is undergoing a digital transformation that introduces new technologies, processes, and business models. Identification of risk involves determining the sources, causes, and potential consequences of IT-related risks that may affect the organization's objectives, assets, and stakeholders. Identification of risk also helps to establish the risk context, scope, and criteria for the subsequent risk analysis, evaluation, and treatment. Without identifying the risks, the information security manager cannot effectively assess the risk exposure, prioritize the

risks, implement appropriate controls, monitor the risk performance, or communicate the risk information to the relevant parties.
Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, page 841; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 34, page 352.

Question: 34

Which of the following BEST ensures timely and reliable access to services?

A. Nonrepudiation
B. Authenticity
C. Availability
D. Recovery time objective (RTO)

Answer: C

Explanation:

= According to the CISM Review Manual, availability is the degree to which information and systems are accessible to authorized users in a timely and reliable manner1. Availability ensures that services are delivered to the users as expected and agreed upon. Nonrepudiation is the ability to prove the occurrence of a claimed event or action and its originating entities1. It ensures that the parties involved in a transaction cannot deny

their involvement. Authenticity is the quality or state of being genuine or original, rather than a reproduction or fabrication1. It ensures that the identity of a subject or resource is valid. Recovery time objective (RTO) is the maximum acceptable period of time that can elapse before the unavailability of a business function severely impacts the organization1. It is a metric used to measure the recovery capability of a system or service, not a factor that ensures timely and reliable access to services. Reference = CISM Review Manual, 16th Edition, Chapter 2, Information Risk Management, pages 66-67.

Question: 35

Which of the following is MOST helpful for determining which information security policies should be implemented by an organization?

A. Risk assessment
B. Business impact analysis (BIA)
C. Vulnerability assessment
D. Industry best practices

Answer: A

Explanation:

Information security policies are high-level statements or rules that define the goals and objectives of information security in an organization, and provide the framework and direction for implementing and enforcing security controls and processes1. Information security policies should be aligned with the organization's business goals and objectives, and reflect the organization's risk appetite and tolerance2. Therefore, the most helpful activity for determining which information security policies should be implemented by an organization is a risk assessment.

A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses3. A risk assessment helps to determine the following aspects of information security policies:

The scope and applicability of the policies, based on the assets, threats, and vulnerabilities that affect the organization's security objectives and requirements.

The level and type of security controls and processes that are needed to mitigate the risks, based on the likelihood and impact of the risk scenarios and the cost-benefit analysis of the risk responses. The roles and responsibilities of the stakeholders involved in the implementation and enforcement of the policies, based on the risk ownership and accountability.

The metrics and indicators that are used to measure and monitor the effectiveness and compliance of the policies, based on the risk appetite and tolerance.

The other options, such as a business impact analysis (BIA), a vulnerability assessment, or industry best practices, are not as helpful as a risk assessment for determining which information security policies should be implemented by an organization, because they have the following limitations: A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of disruptions or incidents on the organization's critical business functions and processes, and determining the recovery priorities and objectives. A BIA can help to support the risk assessment by providing information on the impact and criticality of the assets and processes, but it cannot identify or analyze the threats and vulnerabilities that pose risks to the organization, or determine the appropriate risk responses or controls.

A vulnerability assessment is a process of identifying and measuring the weaknesses or flaws in the

organization's systems, networks, or applications that could be exploited by threat actors. A vulnerability assessment can help to support the risk assessment by providing information on the vulnerabilities and exposures that affect the organization's security posture, but it cannot identify or analyze the threats or likelihood that could exploit the vulnerabilities, or determine the appropriate risk responses or controls. Industry best practices are the standards or guidelines that are widely accepted and followed by the information security community or the organization's industry sector, based on the experience and knowledge of the experts and practitioners. Industry best practices can help to inform and guide the development and implementation of information security policies, but they cannot replace or substitute the risk assessment, as they may not reflect the organization's specific context, needs, and objectives, or address the organization's unique risks and challenges.

Reference = 1: CISM Review Manual 15th Edition, page 29 2: CISM Review Manual 15th Edition, page 30 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 : CISM Review Manual 15th Edition, page 126

Question: 36

The MOST important reason for having an information security manager serve on the change management committee is to:

A. identify changes to the information security policy.
B. ensure that changes are tested.
C. ensure changes are properly documented.
D. advise on change-related risk.

Answer: D

Explanation:

The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts1. Change- related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction2. The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies3. Therefore, the information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes4.

The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The

information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks5. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes. Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities. However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk. Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are

properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change- related risk. Reference = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

Question: 37

Which of the following parties should be responsible for determining access levels to an application that processes client information?

A. The business client
B. The information security tear
C. The identity and access management team
D. Business unit management

Answer: D

Explanation:

The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.
The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information,

but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies. Reference = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

Question: 38

Which of the following provides the BEST assurance that security policies are applied across business operations?

A. Organizational standards are included in awareness training.
B. Organizational standards are enforced by technical controls.
C. Organizational standards are required to be formally accepted.
D. Organizational standards are documented in operational procedures.

Answer: D

Explanation:

= The best assurance that security policies are applied across business operations is that organizational standards are documented in operational procedures. Operational procedures are the specific steps and actions that need to be taken to implement and comply with the security policies and standards. They provide clear and consistent guidance for the staff members who are responsible for performing the security tasks and functions. They also help to ensure that the security policies and standards are aligned with the business objectives and processes, and that they are measurable and auditable. Documenting the organizational standards in operational procedures can help to improve the security awareness, accountability, and performance of the staff members, and to reduce the risks of errors, deviations, and violations. The other options are not the best assurance because they are either too general or too specific. Organizational standards are included in awareness training (A) is a good practice to educate the staff members about the security policies and standards, but it does not guarantee that they will follow them or understand how to apply them in their daily operations. Organizational standards are enforced by technical controls (B) is a way to automate and monitor the compliance with the security policies and standards, but it does not cover all the aspects of security that may require human intervention or judgment. Organizational standards are required to be formally accepted © is a way to obtain the commitment and support from the staff members for the security policies and standards, but it does not ensure that they will adhere to them or know how to execute them in their work activities. Reference = CISM Review Manual 2022, pages 24-25, 28-29; CISM Item Development Guide 2022, page 9; Policies, Procedures, Standards, Baselines, and Guidelines | CISSP Security-Management Practices | Pearson IT Certification

Question: 39

Which of the following will have the GREATEST influence on the successful adoption of an information security governance program?

A. Security policies
B. Control effectiveness
C. Security management processes
D. Organizational culture

Answer: D

Explanation:

Organizational culture is the set of shared values, beliefs, and norms that influence the way employees think, feel, and behave in the workplace. It affects how employees perceive the importance of information security, how they comply with security policies and procedures, and how they support security initiatives and goals. A strong security culture can foster a sense of ownership, responsibility, and accountability among employees, as well as a positive attitude toward security awareness and training. A weak security culture can lead to resistance, indifference, or hostility toward security efforts, as well as increased risks of human errors, negligence, or malicious actions. Therefore, organizational culture has the greatest influence on the successful adoption of an information security governance program, which requires the commitment and involvement of all levels of the organization. Reference = CISM Review Manual 15th Edition, page 30-31.

Learn more:

Question: 40

An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

A. Integrate information security risk assessments into the procurement process.
B. Provide regular information security training to the procurement team.
C. Invite IT members into regular procurement team meetings to influence best practice.
D. Enforce the right to audit in procurement contracts with SaaS vendors.

Answer: A

Explanation:

The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization. Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle. Providing regular information security training to the procurement team (B) is a good practice, but it may not

be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.

Inviting IT members into regular procurement team meetings to influence best practice © is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.

Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts.

Reference = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, Page 141-1421

Question: 41

Which of the following will result in the MOST accurate controls assessment?

A. Mature change management processes
B. Senior management support
C. Well-defined security policies
D. Unannounced testing

Answer: D

Explanation:

Unannounced testing is the most accurate way to assess the effectiveness of controls, as it simulates a real-world scenario and does not allow the staff to prepare or modify their behavior in advance. Mature change management processes, senior management support, and well-defined security policies are all important factors for establishing and maintaining a strong security posture, but they do not directly measure the performance of controls. Reference = CISM Review Manual, 16th Edition, page 149. CISM Questions, Answers & Explanations Database, question ID 1003.

Question: 42

An information security manager learns of a new standard related to an emerging technology the organization wants to implement. Which of the following should the information security manager recommend be done FIRST?

A. Determine whether the organization can benefit from adopting the new standard.
B. Obtain legal counsel's opinion on the standard's applicability to regulations,

C. Perform a risk assessment on the new technology.
D. Review industry specialists' analyses of the new standard.

Answer: A

Explanation:

= The first step that the information security manager should recommend when learning of a new standard related to an emerging technology is to determine whether the organization can benefit from adopting the new standard. This involves evaluating the business objectives, needs, and requirements of the organization, as well as the potential advantages, disadvantages, and challenges of implementing the new technology and the new standard. The information security manager should also consider the alignment of the new standard with the organization's existing policies, procedures, and standards, as well as the impact of the new standard on the organization's information security governance, risk management, program, and incident management. By conducting a preliminary analysis of the feasibility, suitability, and desirability of the new standard, the information security manager can provide a sound basis for further decision making and planning.
Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Standards, page 391; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 43, page 412.

Question: 43

When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?

A. Data is encrypted in transit and at rest at the vendor site.
B. Data is subject to regular access log review.
C. The vendor must be able to amend data.
D. The vendor must agree to the organization's information security policy,

Answer: D

Explanation:

When granting remote access to confidential information to a vendor, the most important security consideration is to ensure that the vendor complies with the organization's information security policy. The information security policy defines the roles, responsibilities, rules, and standards for accessing, handling, and protecting the organization's information assets. The vendor must agree to the policy and sign a contract that specifies the terms and conditions of the access, the security controls to be implemented, the monitoring and auditing mechanisms, the incident reporting and response procedures, and the penalties for non-compliance or breach. The policy also establishes the organization's right to revoke the access at any time if the vendor violates the policy or poses a risk to the organization.
Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Policies, page 34; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 44, page 45.

Question: 44

An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?

A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.

Answer: D

Explanation:

The best course of action when the organization receives complaints from users that some of their files have been encrypted and they are receiving demands for money to decrypt the files is to initiate incident response. This is because the organization is facing a ransomware attack, which is a type of malicious software that encrypts the victim's data and demands a ransom for the decryption key. Ransomware attacks can cause significant disruption, damage, and loss to the organization's operations, assets, and reputation. Therefore, the organization needs to quickly activate its incident response plan and team, which are designed to handle such security incidents in a coordinated, effective, and efficient manner. The incident response process involves the following steps1: Preparation: The incident response team prepares the necessary resources, tools, and procedures to respond to the incident. The team also establishes the roles, responsibilities, and communication channels among the team members and other stakeholders.
Identification: The incident response team identifies the scope, source, and severity of the incident. The team also collects and preserves the relevant evidence and logs for further analysis and investigation.
Containment: The incident response team isolates the affected systems and networks to prevent the spread of the ransomware and limit the impact of the incident. The team also implements temporary or alternative solutions to restore the essential functions and services.
Eradication: The incident response team removes the ransomware and any traces of its infection from the affected systems and networks. The team also verifies that the systems and networks are clean and secure before restoring them to normal operations.
Recovery: The incident response team restores the affected systems and networks to normal operations. The team also decrypts or restores the encrypted data from backups or other sources, if possible. The team also monitors the systems and networks for any signs of recurrence or residual issues.
Lessons learned: The incident response team conducts a post-incident review to evaluate the effectiveness and efficiency of the incident response process and team. The team also identifies the root causes, lessons learned, and best practices from the incident. The team also recommends and implements the necessary improvements and corrective actions to prevent or mitigate similar incidents in the future.
Reference = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, pages 229-2331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 45, page 432.

Question: 45

In which cloud model does the cloud service buyer assume the MOST security responsibility?

A. Disaster Recovery as a Service (DRaaS)
B. Infrastructure as a Service (IaaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)

Answer: B

Explanation:

Infrastructure as a Service (IaaS) is a cloud model in which the cloud service provider (CSP) offers the basic computing resources, such as servers, storage, network, and virtualization, as a service over the internet. The cloud service buyer (CSB) is responsible for installing, configuring, managing, and securing the operating systems, applications, data, and middleware on top of the infrastructure. Therefore, the CSB assumes the most security responsibility in the IaaS model, as it has to protect the confidentiality, integrity, and availability of its own assets and information in the cloud environment. In contrast, in the other cloud models, the CSP takes over more security responsibility from the CSB, as it provides more layers of the service stack. In Disaster Recovery as a Service (DRaaS), the CSP offers the replication and recovery of the CSB's data and applications in the event of a disaster. In Platform as a Service (PaaS), the CSP offers the development and deployment tools, such as programming languages, frameworks, libraries, and databases, as a service. In Software as a Service (SaaS), the CSP offers the complete software applications, such as email, CRM, or ERP, as a service. In these models, the CSB has less control and visibility over the underlying infrastructure, platform, or software, and has to rely on the CSP's security measures and contractual agreements.
Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, page 140-1411

Question: 46

In a business proposal, a potential vendor promotes being certified for international security standards as a measure of its security capability.
Before relying on this certification, it is MOST important that the information security manager confirms that the:

A. current international standard was used to assess security processes.
B. certification will remain current through the life of the contract.
C. certification scope is relevant to the service being offered.
D. certification can be extended to cover the client's business.

Answer: C

Explanation:

Before relying on a vendor's certification for international security standards, such as ISO/IEC 27001, it is most important that the information security manager confirms that the certification scope is relevant to the service being offered. The certification scope defines the boundaries and applicability of the information security management system (ISMS) that the vendor has implemented and audited. The scope should cover the

processes, activities, assets, and locations that are involved in delivering the service to the client. If the scope is too narrow, too broad, or not aligned with the service, the certification may not provide sufficient assurance of the vendor's security capability and performance.

The current international standard was used to assess security processes (A) is an important factor, but not the most important one. The information security manager should verify that the vendor's certification is based on the latest version of the standard, which reflects the current best practices and requirements for information security. However, the standard itself is generic and adaptable, and does not prescribe specific security controls or solutions. Therefore, the certification does not guarantee that the vendor has implemented the most appropriate or effective security processes for the service being offered.

The certification will remain current through the life of the contract (B) is also an important factor, but not the most important one. The information security manager should ensure that the vendor's certification is valid and up to date, and that the vendor maintains its compliance with the standard throughout the contract period. However, the certification is not a one-time event, but a continuous process that requires periodic surveillance audits and recertification every three years. Therefore, the certification does not ensure that the vendor's security capability and performance will remain consistent or satisfactory for the duration of the contract.

The certification can be extended to cover the client's business (D) is not a relevant factor, as the certification is specific to the vendor's ISMS and does not apply to the client's business. The information security manager should not rely on the vendor's certification to substitute or supplement the client's own security policies, standards, or controls. The information security manager should conduct a due diligence and risk assessment of the vendor, and establish a clear and comprehensive service level agreement (SLA) that defines the security roles, responsibilities, expectations, and metrics for both parties.

Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, page 142-1431

Question: 47

Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

A. Management's business goals and objectives
B. Strategies of other non-regulated companies
C. Risk assessment results
D. Industry best practices and control recommendations

Answer: A

Explanation:

When a new information security manager is developing an information security strategy for a nonregulated organization, reviewing the management's business goals and objectives would be the most helpful. This is because the information security strategy should be aligned with and support the organization's vision, mission, values, and strategic direction. The information security strategy should also enable the organization to achieve its desired outcomes, such as increasing revenue, reducing costs, enhancing customer satisfaction, or improving operational efficiency. By reviewing the management's business goals and objectives, the information security manager can understand the business context, needs, and expectations of the

organization, and design the information security strategy accordingly. The information security manager can also communicate the value proposition and benefits of the information security strategy to the management and other stakeholders, and gain their support and commitment.
Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy, page 211; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 48, page 452.

Question: 48

When investigating an information security incident, details of the incident should be shared:

A. widely to demonstrate positive intent.
B. only with management.
C. only as needed,
D. only with internal audit.

Answer: C

Explanation:

When investigating an information security incident, details of the incident should be shared only as needed, according to the principle of least privilege and the need-to-know basis. This means that only the authorized and relevant parties who have a legitimate purpose and role in the incident response process should have access to the incident information, and only to the extent that is necessary for them to perform their duties. Sharing incident details only as needed helps to protect the confidentiality, integrity, and availability of the incident information, as well as the privacy and reputation of the affected individuals and the organization. Sharing incident details only as needed also helps to prevent unauthorized disclosure, modification, deletion, or misuse of the incident information, which could compromise the investigation, evidence, remediation, or legal actions.
Reference = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, page 2311; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 49, page 462.

Question: 49

Which of the following should be the PRIMARY consideration when developing an incident response plan?

A. The definition of an incident
B. Compliance with regulations
C. Management support
D. Previously reported incidents

Answer: B

Explanation:

Management support is the primary consideration when developing an incident response plan, as it is essential for obtaining the necessary resources, authority, and commitment for the plan. Management support also helps to ensure that the plan is aligned with the organization's business objectives, risk appetite, and security strategy, and that it is communicated and enforced across the organization. Management support also facilitates the coordination and collaboration among different stakeholders, such as business units, IT functions, legal, public relations, and external parties, during an incident response.

The definition of an incident (A) is an important component of the incident response plan, as it provides the criteria and thresholds for identifying, classifying, and reporting security incidents. However, the definition of an incident is not the primary consideration, as it is derived from the organization's security policies, standards, and procedures, and may vary depending on the context and impact of the incident.

Compliance with regulations (B) is also an important factor for the incident response plan, as it helps to ensure that the organization meets its legal and contractual obligations, such as notifying the authorities, customers, or partners of a security breach, preserving the evidence, and reporting the incident outcomes. However, compliance with regulations is not the primary consideration, as it is influenced by the nature and scope of the incident, and the applicable laws and regulations in different jurisdictions.

Previously reported incidents (D) are a valuable source of information and lessons learned for the incident response plan, as they help to identify the common types, causes, and impacts of security incidents, as well as the strengths and weaknesses of the current incident response processes and capabilities. However, previously reported incidents are not the primary consideration, as they are not predictive or comprehensive of the future incidents, and may not reflect the changing threat landscape and business environment.

Reference = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 181-1821

Learn more:

Question: 50

An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?

A. Instruct IT to deploy controls based on urgent business needs.
B. Present a business case for additional controls to senior management.
C. Solicit bids for compensating control products.
D. Recommend a different application.

Answer: B

Explanation:

The information security manager should present a business case for additional controls to senior management, as this is the most effective way to communicate the risk and the need for mitigation. The information security manager should not instruct IT to deploy controls based on urgent business needs, as this

may not align with the business objectives and may cause unnecessary costs and delays. The information security manager should not solicit bids for compensating control products, as this may not address the root cause of the risk and may not be the best solution. The information security manager should not recommend a different application, as this may not be feasible or desirable for the business. Reference = CISM Review Manual 2023, page 711; CISM Review Questions, Answers & Explanations Manual 2023, page 252

Question: 51

Which of the following activities MUST be performed by an information security manager for change requests?

A. Perform penetration testing on affected systems.
B. Scan IT systems for operating system vulnerabilities.
C. Review change in business requirements for information security.
D. Assess impact on information security risk.

Answer: D

Explanation:

Question: 52

The effectiveness of an information security governance framework will BEST be enhanced if:

A. consultants review the information security governance framework.
B. a culture of legal and regulatory compliance is promoted by management.
C. risk management is built into operational and strategic activities.
D. IS auditors are empowered to evaluate governance activities

Answer: B

Explanation:

The effectiveness of an information security governance framework will best be enhanced if risk management is built into operational and strategic activities. This is because risk management is a key component of information security governance, which is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed and measured. Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating information security risks that may affect the organization's objectives, assets, and stakeholders. By integrating risk management into operational and strategic activities, the organization can ensure that information security risks are considered and addressed in every decision and action, and that the information security governance framework is aligned with the organization's risk appetite and tolerance. This also helps to optimize the allocation of resources, enhance the performance and value of information security, and improve the accountability and transparency of information security governance.

Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Governance Framework, page 181; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Management, page 812; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 53, page 493.

Question: 53

The BEST way to identify the risk associated with a social engineering attack is to:

A. monitor the intrusion detection system (IDS),
B. review single sign-on (SSO) authentication lags.
C. test user knowledge of information security practices.
D. perform a business risk assessment of the email filtering system.

Answer: C

Explanation:

The best way to identify the risk associated with a social engineering attack is to test user knowledge of information security practices. Social engineering is a type of attack that exploits human psychology and behavior to manipulate, deceive, or influence users into divulging sensitive information, granting unauthorized access, or performing malicious actions. Therefore, user knowledge of information security practices is a key factor that affects the likelihood and impact of a social engineering attack. By testing user knowledge of information security practices, such as through quizzes, surveys, or simulated attacks, the information security manager can measure the level of awareness, understanding, and compliance of the users, and identify the gaps, weaknesses, or vulnerabilities that need to be addressed.

Monitoring the intrusion detection system (IDS) (A) is a possible way to detect a social engineering attack, but not to identify the risk associated with it. An IDS is a system that monitors network or system activities and alerts or responds to any suspicious or malicious events. However, an IDS may not be able to prevent or recognize all types of social engineering attacks, especially those that rely on human interaction, such as phishing, vishing, or baiting. Moreover, monitoring the IDS is a reactive rather than proactive approach, as it only reveals the occurrence or consequences of a social engineering attack, not the potential or likelihood of it.

Reviewing single sign-on (SSO) authentication lags (B) is not a relevant way to identify the risk associated with a social engineering attack. SSO is a method of authentication that allows users to access multiple applications or systems with one set of credentials. Authentication lags are delays or failures in the authentication process that may affect the user experience or performance. However, authentication lags are not directly related to social engineering attacks, as they do not indicate the user's knowledge of information security practices, nor the attacker's attempts or success in compromising the user's credentials or access.

Performing a business risk assessment of the email filtering system (D) is also not a relevant way to identify the risk associated with a social engineering attack. An email filtering system is a system that scans, filters, and blocks incoming or outgoing emails based on predefined rules or criteria, such as spam, viruses, or phishing. A business risk assessment is a process that evaluates the potential threats, vulnerabilities, and impacts to the organization's business objectives, processes, and assets. However, performing a business risk assessment of the email filtering system does not address the risk associated with a social engineering attack, as it only focuses on the technical aspects and performance of the system, not the human factors and behavior of the users.

Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk

Identification, Subsection: Threat Identification, page 87-881

Question: 54

Which of the following is MOST critical when creating an incident response plan?

A. Identifying vulnerable data assets
B. Identifying what constitutes an incident
C. Documenting incident notification and escalation processes
D. Aligning with the risk assessment process

Answer: C

Explanation:

= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures.
Reference = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

Question: 55

Which is the BEST method to evaluate the effectiveness of an alternate processing site when continuous uptime is required?

A. Parallel test
B. Full interruption test
C. Simulation test
D. Tabletop test

Answer: A

Explanation:

A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required. A parallel test involves processing the same transactions or data at both the primary and the alternate site simultaneously, and comparing the results for accuracy and consistency. A parallel test can validate the functionality, performance, and reliability of the alternate site without disrupting the normal operations at the primary site. A parallel test can also identify and resolve any issues or discrepancies between the two sites before a real disaster occurs. A parallel test can provide a high level of assurance and confidence that the alternate site can support the organization's continuity requirements.
Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP) Testing, page 1861; CISM Review Questions, Answers &

Explanations Manual, 10th Edition, Question 56, page 522.

A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required because it involves processing data at both the primary and alternate sites simultaneously without disrupting the normal operations1. A full interruption test would cause downtime and potential loss of data or revenue2. A simulation test would not provide a realistic assessment of the alternate site's capabilities3. A tabletop test would only involve a discussion of the procedures and scenarios without actually testing the site4.

1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM - ISACA Certified Information Security Manager Exam Prep - NICCS 3: Prepare for the ISACA Certified Information Security Manager Exam: CISM … 4: CISM: Certified Information Systems Manager | Official ISACA … - NICCS

Question: 56

How does an incident response team BEST leverage the results of a business impact analysis (BIA)?

A. Assigning restoration priority during incidents
B. Determining total cost of ownership (TCO)
C. Evaluating vendors critical to business recovery
D. Calculating residual risk after the incident recovery phase

Answer: A

Explanation:

The incident response team can best leverage the results of a business impact analysis (BIA) by assigning restoration priority during incidents. A BIA is a process that identifies and evaluates the criticality and dependency of the organization's business functions, processes, and resources, and the potential impacts and consequences of their disruption or loss. The BIA results provide the basis

for determining the recovery objectives, strategies, and plans for the organization's business continuity and disaster recovery. By using the BIA results, the incident response team can prioritize the restoration of the most critical and time-sensitive business functions, processes, and resources, and allocate the appropriate resources, personnel, and time to minimize the impact and duration of the incident.

Determining total cost of ownership (TCO) (B) is not a relevant way to leverage the results of a BIA, as it is not directly related to incident response. TCO is a financial metric that estimates the total direct and indirect costs of owning and operating an asset or a system over its lifecycle. TCO may be useful for evaluating the cost-effectiveness and return on investment of different security solutions or alternatives, but it does not help the incident response team to respond to or recover from an incident.

Evaluating vendors critical to business recovery © is also not a relevant way to leverage the results of a BIA, as it is not a primary responsibility of the incident response team. Evaluating vendors critical to business recovery is a part of the vendor management process, which involves selecting, contracting, monitoring, and reviewing the vendors that provide essential products or services to support the organization's business continuity and disaster recovery. Evaluating vendors critical to business recovery may be done before or after an incident, but not during an incident, as it does not contribute to the incident response or restoration activities.

Calculating residual risk after the incident recovery phase (D) is also not a relevant way to leverage the results

of a BIA, as it is not a timely or effective use of the BIA results. Residual risk is the risk that remains after the implementation of risk treatment or mitigation measures. Calculating residual risk after the incident recovery phase may be done as a part of the incident review or improvement process, but not during the incident response or restoration phase, as it does not help the incident response team to resolve or contain the incident.

Reference = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Business Impact Analysis, page 182-1831

Question: 57

Which of the following is MOST important to consider when determining asset valuation?

A. Asset recovery cost
B. Asset classification level
C. Cost of insurance premiums
D. Potential business loss

Answer: D

Explanation:

Potential business loss is the most important factor to consider when determining asset valuation, as it reflects the impact of losing or compromising the asset on the organization's objectives and operations. Asset recovery cost, asset classification level, and cost of insurance premiums are also relevant, but not as important as potential business loss, as they do not capture the full value of the asset to the organization. Reference = CISM Review Manual 2023, page 461; CISM Review Questions, Answers & Explanations Manual 2023, page 292

Question: 58

An information security manager learns that IT personnel are not adhering to the information security policy because it creates process inefficiencies. What should the information security manager do FIRST?

A. Conduct user awareness training within the IT function.
B. Propose that IT update information security policies and procedures.
C. Determine the risk related to noncompliance with the policy.
D. Request that internal audit conduct a review of the policy development process,

Answer: C

Explanation:

The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes,

or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

Question: 59

Which of the following is the BEST indication ofa successful information security culture?

A. Penetration testing is done regularly and findings remediated.
B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.

Answer: B

Explanation:

The best indication of a successful information security culture is that end users know how to identify and report incidents. This shows that the end users are aware of the information security policies, procedures, and practices of the organization, and that they understand their roles and responsibilities in protecting the information assets and resources. It also shows that the end users are engaged and committed to the information security goals and objectives of the organization, and that they are willing to cooperate and collaborate with the information security team and other

stakeholders in preventing, detecting, and responding to information security incidents. A successful information security culture is one that fosters a positive attitude and behavior toward information security among all members of the organization, and that aligns the information security strategy with the business strategy and the organizational culture1.

Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281.

Question: 60

An organization finds it necessary to quickly shift to a work-fromhome model with an increased need for remote access security.

Which of the following should be given immediate focus?

A. Moving to a zero trust access model
B. Enabling network-level authentication
C. Enhancing cyber response capability
D. Strengthening endpoint security

Answer: D

Explanation:

Strengthening endpoint security is the most immediate focus when shifting to a work-from-home model with an increased need for remote access security, as this reduces the risk of unauthorized access, data leakage, malware infection, and other threats that may compromise the confidentiality, integrity, and availability of the organization's information assets. Moving to a zero trust access model, enabling network-level authentication, and enhancing cyber response capability are also important, but not as urgent as strengthening endpoint security, as they require more time, resources, and planning to implement effectively. Reference = CISM Review Manual 2023, page 1561; CISM Review Questions, Answers & Explanations Manual 2023, page 302; ISACA CISM - iSecPrep, page 153

Question: 61

Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?

A. Defining information stewardship roles
B. Defining security asset categorization
C. Assigning information asset ownership
D. Developing a records retention schedule

Answer: C

Explanation:

The most important factor to ensuring information stored by an organization is protected appropriately is assigning information asset ownership. Information asset ownership is the process of identifying and assigning the roles and responsibilities of the individuals or groups who have the authority and accountability for the information assets and their protection. Information asset owners are responsible for defining the business value, classification, and security requirements of the information assets, as well as granting the access rights and privileges to the information users and custodians. Information asset owners are also responsible for monitoring and reviewing the security performance and compliance of the information assets, and reporting and resolving any security issues or incidents. By assigning information asset ownership, the organization can ensure that the information assets are properly identified, categorized, protected, and managed according to their importance, sensitivity, and regulatory obligations.
Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 62, page 572.

Question: 62

What is the BEST way to reduce the impact of a successful ransomware attack?

A. Perform frequent backups and store them ofline.
B. Purchase or renew cyber insurance policies.

C. Include provisions to pay ransoms ih the information security budget.
D. Monitor the network and provide alerts on intrusions.

Answer: A

Explanation:

Performing frequent backups and storing them ofline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself. Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware. Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. Reference = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

Question: 63

Which of the following would be the BEST way for an information security manager to improve the effectiveness of an organization's information security program?

A. Focus on addressing conflicts between security and performance.

B. Collaborate with business and IT functions in determining controls.
C. Include information security requirements in the change control process.
D. Obtain assistance from IT to implement automated security cantrals.

Answer: B

Explanation:

The best way for an information security manager to improve the effectiveness of an organization's information security program is to collaborate with business and IT functions in determining controls. Collaboration is a key factor for ensuring that the information security program is aligned with the organization's business objectives, risk appetite, and security strategy, and that it supports the business processes and activities. Collaboration also helps to gain the buy-in, involvement, and ownership of the business and IT functions, who are the primary stakeholders and users of the information security program. Collaboration also facilitates the communication, coordination, and integration of the information security program across the organization, and enables the information security manager to understand the needs, expectations, and challenges of the business and IT functions, and to propose the most appropriate and effective security controls and solutions. Focusing on addressing conflicts between security and performance (A) is a possible way to improve the effectiveness of an information security program, but not the best one. Security and performance are often competing or conflicting goals, as security controls may introduce overhead, complexity, or delays that affect the efficiency, usability, or availability of the systems or processes. Addressing these conflicts may help to optimize the balance and trade-off between security and performance,

and to enhance the user satisfaction and acceptance of the security controls. However, focusing on addressing conflicts between security and performance does not necessarily improve the alignment, integration, or communication of the information security program with the business and IT functions, nor does it ensure the involvement or ownership of the stakeholders.

Including information security requirements in the change control process © is also a possible way to improve the effectiveness of an information security program, but not the best one. The change control process is a process that manages the initiation, approval, implementation, and review of changes to the systems or processes, such as enhancements, updates, or fixes. Including information security requirements in the change control process may help to ensure that the changes do not introduce new or increased security risks or impacts, and that they comply with the security policies, standards, and procedures. However, including information security requirements in the change control process does not necessarily improve the collaboration, communication, or coordination of the information security program with the business and IT functions, nor does it ensure the buy-in or involvement of the stakeholders.

Obtaining assistance from IT to implement automated security controls (D) is also a possible way to improve the effectiveness of an information security program, but not the best one. Automated security controls are security controls that are implemented by using software, hardware, or other technologies, such as encryption, firewalls, or antivirus, to perform security functions or tasks without human intervention. Obtaining assistance from IT to implement automated security controls may help to improve the efficiency, consistency, or reliability of the security controls, and to reduce the human errors, negligence, or malicious actions. However, obtaining assistance from IT to implement automated security controls does not necessarily improve the collaboration, communication, or integration of the information security program with the business and IT functions, nor does it ensure the ownership or involvement of the stakeholders.

Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy Development, Subsection: Collaboration, page 24-251

Question: 64

Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To facilitate a qualitative risk assessment following the BIA
B. To increase awareness of information security among key stakeholders
C. To ensure the stakeholders providing input own the related risk
D. To obtain input from as many relevant stakeholders as possible

Answer: D

Explanation:

The most important reason to conduct interviews as part of the business impact analysis (BIA) process is to obtain input from as many relevant stakeholders as possible. A BIA is a process of identifying and analyzing the potential effects of disruptive events on the organization's critical business functions, processes, and resources. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's continuity planning. Interviews are one of the methods to collect data and information for the BIA, and they involve direct and interactive communication with the stakeholders who are involved in or affected by the business functions, processes, and resources. By conducting interviews, the information security manager can obtain input from as many relevant stakeholders as possible, such as business owners, managers, users, customers,

suppliers, regulators, and partners. This can help to ensure that the BIA covers the full scope and complexity of the organization's business activities, and that the BIA reflects the accurate, current, and comprehensive views and expectations of the stakeholders. Interviews can also help to validate, clarify, and supplement the data and information obtained from other sources, such as surveys, questionnaires, documents, or systems. Interviews can also help to build rapport, trust, and collaboration among the stakeholders, and to increase their awareness, involvement, and commitment to the information security and continuity planning.
Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Impact Analysis (BIA), pages 178-1801; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 65, page 602.

Question: 65

Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?

A. To compare emerging trends with the existing organizational security posture
B. To communicate worst-case scenarios to senior management
C. To train information security professionals to mitigate new threats
D. To determine opportunities for expanding organizational information security

Answer: A

Explanation:

The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce the likelihood and impact of cyberattacks. Reference = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

Question: 66

Which of the following is the BEST course of action for an information security manager to align security and business goals?

A. Conducting a business impact analysis (BIA)
B. Reviewing the business strategy
C. Defining key performance indicators (KPIs)
D. Actively engaging with stakeholders

Answer: D

Explanation:

= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them. By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. Reference = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

Question: 67

An information security manager is reporting on open items from the risk register to senior management. Which of the following is MOST important to communicate with regard to these risks?

A. Responsible entities
B. Key risk indicators (KRIS)
C. Compensating controls
D. Potential business impact

Answer: D

Explanation:

The most important information to communicate with regard to the open items from the risk register to senior management is the potential business impact of these risks. The potential business impact is the estimated consequence or loss that the organization may suffer if the risk materializes or occurs. The potential business impact can be expressed in quantitative or qualitative terms, such as financial, operational, reputational, legal, or strategic impact. Communicating the potential business impact of the open items from the risk register helps senior management to understand the severity and urgency of these risks, and to prioritize the risk response actions and resources accordingly. Communicating the potential business impact also helps senior management to align the risk management objectives and activities with the business objectives and strategies, and to ensure that the risk appetite and tolerance of the organization are respected and maintained. Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Reporting, page 1012.

Question: 68

Which of the following would be MOST useful to a newly hired information security manager who has been tasked with developing and implementing an information security strategy?

A. The capabilities and expertise of the information security team
B. The organization's mission statement and roadmap
C. A prior successful information security strategy
D. The organization's information technology (IT) strategy

Answer: B

Explanation:

= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization's mission statement and roadmap. The mission statement defines the organization's purpose, vision, values, and goals, and the roadmap outlines the organization's strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security manager can understand the organization's business objectives, risk appetite, and security needs, and align the information security strategy with them. The information security strategy should support and enable the organization's mission and roadmap, and provide the security governance, policies, standards, and controls to protect the organization's information assets and processes.

The capabilities and expertise of the information security team (A) are important factors for the information security manager to consider, but they are not the most useful source of information for developing and implementing an information security strategy. The information security team is responsible for executing and maintaining the information security program and activities, such as risk management, security awareness, incident response, and compliance. The information security manager should assess the capabilities and expertise of the information security team to identify the strengths, weaknesses, opportunities, and threats, and to plan the resource allocation, training, and development of the team. However, the capabilities and expertise of the information security team do not directly inform the information security strategy, which should be driven by the organization's business objectives, risk appetite, and security needs.

A prior successful information security strategy © is a possible source of information for the information security manager to refer to, but it is not the most useful one. A prior successful information security strategy is a strategy that has been implemented and evaluated by another organization or a previous information security manager, and has achieved the desired security outcomes and benefits. The information security manager can learn from the best practices, lessons learned, and challenges of a prior successful information security strategy, and apply them to the current organization or situation. However, a prior successful information security strategy may not be relevant, applicable, or suitable for the organization, as it may not reflect the current or future business objectives, risk appetite, and security needs of the organization, or the changing threat landscape and business environment.

The organization's information technology (IT) strategy (D) is also a possible source of information for the information security manager to consult, but it is not the most useful one. The IT strategy is a strategy that defines the IT vision, goals, and initiatives of the organization, and how IT supports and enables the business processes and activities. The information security manager should review the IT strategy to understand the IT infrastructure, systems, and services of the organization, and how they relate to the information security program and activities. However, the IT strategy is not the primary driver of the information security strategy, which should be aligned with the organization's business objectives, risk appetite, and security needs, and not only with the IT objectives, capabilities, and requirements.

Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy Development, page 23-241

Question: 69

Which of the following is MOST important when conducting a forensic investigation?

A. Analyzing system memory

B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody

Answer: D

Explanation:

Maintaining a chain of custody is the most important step when conducting a forensic investigation, as this ensures that the evidence is preserved, protected, and documented from the time of collection to the time of presentation in court. A chain of custody provides a record of who handled

the evidence, when, where, why, and how, and prevents any tampering, alteration, or loss of the evidence. A chain of custody also establishes the authenticity, reliability, and admissibility of the evidence in legal proceedings. Analyzing system memory, documenting analysis steps, and capturing full system images are also important, but not as important as maintaining a chain of custody, as they do not guarantee the integrity and validity of the evidence. Reference = CISM Review Manual 2023, page 1701; CISM Review Questions, Answers & Explanations Manual 2023, page 332; ISACA CISM - iSecPrep, page 183

Question: 70

Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?

A. Evaluate privacy technologies required for data protection.
B. Encrypt all personal data stored on systems and networks.
C. Update disciplinary processes to address privacy violations.
D. Create an inventory of systems where personal data is stored.

Answer: D

Explanation:

= The first step when establishing a new data protection program that must comply with applicable data privacy regulations is to create an inventory of systems where personal data is stored. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, email, phone number, identification number, location data, biometric data, or online identifiers. Data privacy regulations are laws and rules that govern the collection, processing, storage, transfer, and disposal of personal data, and that grant rights and protections to the data subjects, such as the right to access, rectify, erase, or restrict the use of their personal data. Examples of data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Creating an inventory of systems where personal data is stored is essential for the data protection program, because it helps to:

Identify the sources, types, and locations of personal data that the organization collects and holds, and the purposes and legal bases for which they are used.

Assess the risks and impacts associated with the personal data, and the compliance requirements and

obligations under the applicable data privacy regulations.

Implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, modification, or loss, such as encryption, pseudonymization, access control, backup, or audit logging.

Establish policies, procedures, and processes to manage the personal data throughout their life cycle, and to respond to the requests and complaints from the data subjects or the data protection authorities.

Monitor and review the performance and effectiveness of the data protection program, and report and resolve any data breaches or incidents.

Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Data Protection, pages 202-2051; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 71, page 662.

Question: 71

Which of the following BEST indicates that information security governance and corporate governance are integrated?

A. The information security team is aware of business goals.

B. The board is regularly informed of information security key performance indicators (KPIs), C. The information security steering committee is composed of business leaders.

D. A cost-benefit analysis is conducted on all information security initiatives.

Answer: C

Explanation:

The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security manager has the support and involvement of the senior management. The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. Reference = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

Question: 72

Which of the following should be the PRIMARY objective of the information security incident response process?

A. Conducting incident triage
B. Communicating with internal and external parties
C. Minimizing negative impact to critical operations
D. Classifying incidents

Answer: C

Explanation:

The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents. The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.

Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed. However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.

Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.

Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.

Reference = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

Question: 73

An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?

A. Red team exercise
B. Black box penetration test

C. Disaster recovery exercise

D. Tabletop exercise

Answer: D

Explanation:

= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low-cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills, and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.

A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A disaster recovery exercise © is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high-risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

Reference = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

Question: 74

Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?

A. Publish adopted information security standards.

B. Perform annual information security compliance reviews.
C. Implement an information security governance framework.
D. Define penalties for information security noncompliance.

Answer: C

Explanation:

The best way to ensure the organization's security objectives are embedded in business operations is to implement an information security governance framework. An information security governance framework is a set of policies, procedures, standards, guidelines, roles, and responsibilities that define and direct how the organization manages and measures its information security activities. An information security governance framework helps to align the information security strategy with the business strategy and the organizational culture, and to ensure that the information security objectives are consistent with the business objectives and the stakeholder expectations. An information security governance framework also helps to establish the authority, accountability, and communication channels for the information security function, and to provide the necessary resources, tools, and controls to implement and monitor the information security program. By implementing an information security governance framework, the organization can embed the information security objectives in business operations, and ensure that the information security function supports and enables the business processes and functions, rather than hinders or restricts them.
Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Governance Framework, page 181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 75, page 702.

Question: 75

Which of the following is the BEST way to achieve compliance with new global regulations related to the protection of personal information?

A. Execute a risk treatment plan.
B. Review contracts and statements of work (SOWs) with vendors.
C. Implement data regionalization controls.
D. Determine current and desired state of controls.

Answer: D

Explanation:

The best way to achieve compliance with new global regulations related to the protection of personal information is to determine the current and desired state of controls, as this helps the information security manager to identify the gaps and requirements for compliance, and to prioritize and implement the necessary actions and measures to meet the regulatory standards. The current state of controls refers to the existing level of protection and compliance of the personal information, while the desired state of controls refers to the target level of protection and compliance that is required by the new regulations. By comparing the current and desired state of controls, the

information security manager can assess the maturity and effectiveness of the information security program, and plan and execute a risk treatment plan to address the risks and issues related to the protection of personal information. Executing a risk treatment plan, reviewing contracts and statements of work (SOWs) with vendors, and implementing data regionalization controls are also important, but not as important as determining the current and desired state of controls, as they are dependent on the outcome of the gap analysis and the risk assessment, and may not be sufficient or appropriate to achieve compliance with the new regulations.
Reference = CISM Review Manual 2023, page 491; CISM Review Questions, Answers & Explanations Manual 2023, page 352; ISACA CISM - iSecPrep, page 203

Question: 76

Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

A. Communicate disciplinary processes for policy violations.
B. Require staff to participate in information security awareness training.
C. Require staff to sign confidentiality agreements.
D. Include information security responsibilities in job descriptions.

Answer: B

Explanation:

The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
Reference = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

Question: 77

An online bank identifies a successful network attack in progress. The bank should FIRST:

A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (PII) is compromised.
D. shut down the entire network.

Answer: A

Explanation:

The online bank should first isolate the affected network segment, as this is the most effective way to contain the attack and prevent it from spreading to other parts of the network or compromising more data or systems. Isolating the affected network segment also helps to preserve the evidence and facilitate the investigation and recovery process. Reporting the root cause to the board of directors, assessing whether personally identifiable information (PII) is compromised, and shutting down the entire network are not the first actions that the online bank should take, as they may not be feasible or appropriate at the time of the attack, and may cause more disruption, confusion, or damage to the business operations and reputation. Reference = CISM Review Manual 2023, page 1641; CISM Review Questions, Answers & Explanations Manual 2023, page 362; ISACA CISM - iSecPrep, page 213

Question: 78

Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.
D. Base mandatory review and exception approvals on inherent risk.

Answer: A

Explanation:

= Residual risk is the risk that remains after applying security controls. It reflects the actual exposure of the organization to noncompliance issues. Therefore, basing mandatory review and exception approvals on residual risk is the best approach for governing noncompliance with security requirements. It ensures that the organization is aware of the potential impact and likelihood of noncompliance and can make informed decisions about accepting, mitigating, or transferring the risk. Reference = CISM Review Manual 15th Edition, page 78.

Question: 79

Which of the following is the PRIMARY role of an information security manager in a software development project?

A. To enhance awareness for secure software design

B. To assess and approve the security application architecture
C. To identify noncompliance in the early design stage
D. To identify software security weaknesses

Answer: B

Explanation:

The primary role of an information security manager in a software development project is to assess and approve the security application architecture. The security application architecture is the design and structure of the software application that defines how the application components interact with each other and with external systems, and how the application implements the security requirements, principles, and best practices. The information security manager is responsible for ensuring that the security application architecture is aligned with the organization's information security policies, standards, and guidelines, and that it meets the business objectives, functional specifications, and user expectations. The information security manager is also responsible for reviewing and evaluating the security application architecture for its completeness, correctness, consistency, and compliance, and for identifying and resolving any security issues, risks, or gaps. The information security manager is also responsible for approving the security application architecture before the software development project proceeds to the next phase, such as coding, testing, or deployment.

Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 80, page 742.

Question: 80

Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?

A. Number of blocked intrusion attempts
B. Number of business cases reviewed by senior management
C. Trends in the number of identified threats to the business
D. Percentage of controls integrated into business processes

Answer: D

Explanation:

Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the

information security policies and standards among the business users. Number of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations.

Reference = CISM Review Manual 2023, page 291; CISM Review Questions, Answers & Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

Question: 81

An organization's marketing department wants to use an online collaboration service, which is not in compliance with the information security policy, A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

A. the chief risk officer (CRO).
B. business senior management.
C. the information security manager.
D. the compliance officer.

Answer: B

Explanation:

Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident. Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel, and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.

The chief risk officer (CRO) (A) is a senior executive who oversees the organization's risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

The information security manager © is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

The compliance officer (D) is the officer who oversees the organization's compliance function, and

provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

Reference = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

Question: 82

Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?

A. Disaster recovery plan (DRP)
B. Incident response plan
C. Business continuity plan (BCP)
D. Business contingency plan

Answer: C

Explanation:

= A business continuity plan (BCP) is the plan that should be invoked by an organization in an effort to remain operational during a disaster. A disaster is a sudden, unexpected, or disruptive event that causes significant damage, loss, or interruption to the organization's normal operations, assets, or resources. Examples of disasters are natural disasters, such as earthquakes, floods, or fires, or human-made disasters, such as cyberattacks, sabotage, or terrorism. A BCP is a document that describes the procedures, strategies, and actions that the organization will take to ensure the continuity of its critical business functions, processes, and services in the event of a disaster. A BCP also defines the roles and responsibilities of the staff, management, and other stakeholders involved in the business continuity management, and the resources, tools, and systems that will support the business continuity activities. A BCP helps the organization to:
Minimize the impact and duration of the disaster on the organization's operations, assets, and reputation.
Restore the essential functions and services as quickly and efficiently as possible.
Protect the health, safety, and welfare of the staff, customers, and partners.
Meet the legal, regulatory, contractual, and ethical obligations of the organization.
Learn from the disaster and improve the business continuity capabilities and readiness of the organization.
Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP), page 1771; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 83, page 772.

Question: 83

A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?

A. The time and location that the breach occurred
B. Evidence of previous incidents caused by the user
C. The underlying reason for the user error
D. Appropriate disciplinary procedures for user error

Answer: C

Explanation:

The underlying reason for the user error is the most important factor to determine during the postincident review, as this helps the information security manager to understand the root cause of the breach, and to implement corrective and preventive actions to avoid similar incidents in the future. The underlying reason for the user error may be related to the lack of training, awareness, guidance, or motivation of the user, or to the complexity, usability, or design of the system or process that the user was using. By identifying the underlying reason for the user error, the information security manager can address the human factor of the information security program, and improve the security culture and behavior of the organization. The time and location that the breach occurred, evidence of previous incidents caused by the user, and appropriate disciplinary procedures for user error are not the most important factors to determine during the post-incident review, as they do not provide a comprehensive and holistic understanding of the breach, and may not help to prevent or reduce the likelihood or impact of future incidents. Reference = CISM Review Manual 2023, page 1671; CISM Review Questions, Answers & Explanations Manual 2023, page 382; ISACA CISM - iSecPrep, page 233

Question: 84

Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?

A. Intrusion detection
B. Log monitoring
C. Patch management
D. Antivirus software

Answer: C

Explanation:

= Patch management is the process of applying updates to software and hardware systems to fix security vulnerabilities and improve functionality. Patch management is one of the best ways to prevent the exploitation of system vulnerabilities, as it reduces the attack surface and closes the gaps that attackers can exploit. Patch management also helps to ensure compliance with security

standards and regulations, and maintain the performance and availability of systems.
Intrusion detection is the process of monitoring network or system activities for signs of malicious or unauthorized behavior. Intrusion detection can help to detect and respond to attacks, but it does not prevent them from happening in the first place. Log monitoring is the process of collecting, analyzing and reviewing log files generated by various systems and applications. Log monitoring can help to identify anomalies, errors and security incidents, but it does not prevent them from occurring.
Antivirus software is the program that scans files and systems for viruses, malware and other malicious code. Antivirus software can help to protect systems from infection, but it does not prevent the exploitation of system vulnerabilities that are not related to malware.
Therefore, patch management is the best security process to prevent the exploitation of system vulnerabilities, as it addresses the root cause of the problem and reduces the risk of compromise. Reference = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section 4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 204.

Question: 85

Which of the following is the FIRST step to establishing an effective information security program?

A. Conduct a compliance review.
B. Assign accountability.
C. Perform a business impact analysis (BIA).
D. Create a business case.

Answer: D

Explanation:

According to the CISM Review Manual, the first step to establishing an effective information security program is to create a business case that aligns the program objectives with the organization's goals and strategies. A business case provides the rationale and justification for the information security program and helps to secure the necessary resources and support from senior management and other stakeholders. A business case should include the following elements:

The scope and objectives of the information security program
The current state of information security in the organization and the gap analysis
The benefits and value proposition of the information security program
The risks and challenges of the information security program
The estimated costs and resources of the information security program
The expected outcomes and performance indicators of the information security program
The implementation plan and timeline of the information security program

Reference = CISM Review Manual, 16th Edition, Chapter 3, Section 2, pages 97-99.

Question: 86

An organization recently outsourced the development of a mission-critical business application.
Which of the following would be the BEST way to test for the existence of backdoors?

A. Scan the entire application using a vulnerability scanning tool.
B. Run the application from a high-privileged account on a test system.
C. Perform security code reviews on the entire application.
D. Monitor Internet traffic for sensitive information leakage.

Answer: C

Explanation:

The best way to test for the existence of backdoors in a mission-critical business application that was outsourced to a third-party developer is to perform security code reviews on the entire application. A backdoor is a hidden or undocumented feature or function in a software application that allows unauthorized or remote access, control, or manipulation of the application or the system it runs on. Backdoors can be intentionally or unintentionally introduced by the developers, or maliciously inserted by the attackers, and they can pose serious security risks and threats to the organization and its data. Security code reviews are the process of

examining and analyzing the source code of a software application to identify and eliminate any security vulnerabilities, flaws, or weaknesses, such as backdoors, that may compromise the functionality, performance, or integrity of the application or the system. Security code reviews can be performed manually by the security experts, or automatically by the security tools, or both, and they can be done at different stages of the software development life cycle, such as design, coding, testing, or deployment. Security code reviews can help to detect and remove any backdoors in the application before they can be exploited by the attackers, and they can also help to improve the quality, reliability, and security of the application. Reference = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 87, page 812; CISM ITEM DEVELOPMENT GUIDE, page 63.

Question: 87

The PRIMARY benefit of introducing a single point of administration in network monitoring is that it:

A. reduces unauthorized access to systems.
B. promotes efficiency in control of the environment.
C. prevents inconsistencies in information in the distributed environment.
D. allows administrative staff to make management decisions.

Answer: B

Explanation:

A single point of administration in network monitoring is a centralized system that allows network administrators to manage and monitor the entire network from one location. A single point of administration can provide several benefits, such as:

Promoting efficiency in control of the environment: A single point of administration can simplify and streamline the network management tasks, such as configuration, troubleshooting, performance optimization, security updates, backup and recovery, etc. It can also reduce the time and cost of network maintenance and administration, as well as improve the consistency and quality of network services.

Reducing unauthorized access to systems: A single point of administration can enhance the network security by implementing centralized authentication, authorization and auditing mechanisms. It can also enforce consistent security policies and standards across the network, and detect and respond to any unauthorized or malicious activities.

Preventing inconsistencies in information in the distributed environment: A single point of administration can ensure the data integrity and availability by synchronizing and replicating the data across the network nodes. It can also provide a unified view of the network status and performance, and facilitate the analysis and reporting of network data.

Allowing administrative staff to make management decisions: A single point of administration can support the decision-making process by providing relevant and timely information and feedback to the network administrators. It can also enable the administrators to implement changes and improvements to the network based on the business needs and objectives.

Therefore, the primary benefit of introducing a single point of administration in network monitoring is that it promotes efficiency in control of the environment, as it simplifies and streamlines the network management tasks and improves the network performance and quality. Reference = CISM Review Manual, 16th Edition

Watermark Sample

eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section 4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 205.

Question: 88

Due to changes in an organization's environment, security controls may no longer be adequate. What is the information security manager's BEST course of action?

A. Review the previous risk assessment and countermeasures.
B. Perform a new risk assessment,
C. Evaluate countermeasures to mitigate new risks.
D. Transfer the new risk to a third party.

Answer: B

Explanation:

According to the CISM Review Manual, the information security manager's best course of action when security controls may no longer be adequate due to changes in the organization's environment is to perform a new risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the risks that affect the organization's information assets and business processes. A risk assessment should be performed periodically or whenever there are significant changes in the organization's environment, such as new threats, vulnerabilities, technologies, regulations, or business objectives. A risk assessment helps to determine the current level of risk exposure and the adequacy of existing security controls. A risk assessment also provides the basis for developing or updating the risk treatment plan, which defines the appropriate risk responses, such as

implementing new or enhanced security controls, transferring the risk to a third party, accepting the risk, or avoiding the risk.

The other options are not the best course of action in this scenario. Reviewing the previous risk assessment and countermeasures may not reflect the current state of the organization's environment and may not identify new or emerging risks. Evaluating countermeasures to mitigate new risks may be premature without performing a new risk assessment to identify and prioritize the risks. Transferring the new risk to a third party may not be feasible or cost-effective without performing a new risk assessment to evaluate the risk level and the available risk transfer options. Reference = CISM Review Manual, 16th Edition, Chapter 2, Section 1, pages 43-45.

Question: 89

Which of the following is the BEST indication of an effective information security awareness training program?

A. An increase in the frequency of phishing tests
B. An increase in positive user feedback
C. An increase in the speed of incident resolution
D. An increase in the identification rate during phishing simulations

Answer: D

Explanation:

An effective information security awareness training program should aim to improve the knowledge, skills and behavior of the employees regarding information security. One of the ways to measure the effectiveness of such a program is to conduct phishing simulations, which are mock phishing attacks that test the employees' ability to identify and report phishing emails. An increase in the identification rate during phishing simulations indicates that the employees have learned how to recognize and avoid phishing attempts, which is one of the common threats to information security. Therefore, this is the best indication of an effective information security awareness training program among the given options.

The other options are not as reliable or relevant as indicators of an effective information security awareness training program. An increase in the frequency of phishing tests does not necessarily mean that the employees are learning from them or that the tests are aligned with the learning objectives of the program. An increase in positive user feedback may reflect the satisfaction or engagement of the employees with the program, but it does not measure the actual learning outcomes or behavior changes. An increase in the speed of incident resolution may be influenced by other factors, such as the availability and efficiency of the incident response team, the severity and complexity of the incidents, or the tools and processes used for incident management. Moreover, the speed of incident resolution does not reflect the prevention or reduction of incidents, which is a more desirable goal of an information security awareness training program. Reference = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1001.

Question: 90

Which of the following BEST helps to ensure a risk response plan will be developed and executed in a timely manner?

A. Establishing risk metrics
B. Training on risk management procedures
C. Reporting on documented deficiencies
D. Assigning a risk owner

Answer: D

Explanation:

Assigning a risk owner is the best way to ensure a risk response plan will be developed and executed in a timely manner, because a risk owner is responsible for monitoring, controlling, and reporting on the risk, as well as implementing the appropriate risk response actions. A risk owner should have the authority, accountability, and resources to manage the risk effectively. Establishing risk metrics, training on risk management procedures, and reporting on documented deficiencies are all important aspects of risk management, but they do not guarantee that a risk response plan will be executed promptly and properly. Risk metrics help to measure and communicate the risk level and performance, but they do not assign any responsibility or action. Training on risk management procedures helps to increase the awareness and competence of the staff involved in risk management, but it does not ensure that they will follow the procedures or have the authority to do so. Reporting on documented deficiencies helps to identify and communicate the gaps and weaknesses in the risk management process, but it does not provide any solutions or corrective actions. Reference = CISM Review

Manual, 16th Edition, ISACA, 2021, pages 125-126, 136-137.

Question: 91

Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

A. Providing ongoing training to the incident response team
B. Implementing proactive systems monitoring
C. Implementing a honeypot environment
D. Updating information security awareness materials

Answer: B

Explanation:

= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack,

as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.

Reference = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

Question: 92

Which of the following is MOST important in increasing the effectiveness of incident responders?

A. Communicating with the management team
B. Integrating staff with the IT department
C. Testing response scenarios
D. Reviewing the incident response plan annually

Answer: C

Explanation:

= Testing response scenarios is the most important factor in increasing the effectiveness of incident responders, as it allows them to practice their skills, identify gaps and weaknesses, evaluate the adequacy and feasibility of the incident response plan, and improve their coordination and communication. Testing response scenarios can also help to enhance the confidence and readiness of the incident responders, as well as to measure their performance and compliance with the policies and procedures. Testing response scenarios can be done through various methods, such as tabletop exercises, simulations, drills, or full-scale exercises,

depending on the scope, objectives, and complexity of the scenarios.

The other options are not as important as testing response scenarios, although they may also contribute to the effectiveness of incident responders. Communicating with the management team is important to ensure that the incident responders have the necessary support, resources, and authority to carry out their tasks, as well as to report the status and outcomes of the incident response. However, communication alone is not sufficient to increase the effectiveness of incident responders, as they also need to have the relevant knowledge, skills, and experience to handle the incidents. Integrating staff with the IT department may help to facilitate the collaboration and information sharing between the incident responders and the IT staff, who may have the technical expertise and access to the systems and data involved in the incidents. However, integration alone is not enough to increase the effectiveness of incident responders, as they also need to have the appropriate roles, responsibilities, and processes to manage the incidents. Reviewing the incident response plan annually is important to ensure that the plan is updated and aligned with the current risks, threats, and business requirements, as well as to incorporate the lessons learned and best practices from previous incidents. However, reviewing the plan alone is not enough to increase the effectiveness of incident responders, as they also need to test and validate the plan in realistic scenarios and conditions. Reference = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 223-225, 230-231.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1004.

Question: 93

Which of the following activities is designed to handle a control failure that leads to a breach?

A. Risk assessment
B. Incident management
C. Root cause analysis
D. Vulnerability management

Answer: B

Explanation:

Incident management is the activity designed to handle a control failure that leads to a breach. Incident management is the process of identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. Incident management aims to minimize the impact of a breach, restore normal operations as quickly as possible, and prevent or reduce the likelihood of recurrence. Incident management involves several steps, such as:

Establishing an incident response team with clear roles and responsibilities

Developing and maintaining an incident response plan that defines the procedures, tools, and resources for handling incidents

Implementing detection and reporting mechanisms to identify and communicate incidents Performing triage and analysis to assess the scope, severity, and root cause of incidents Containing and eradicating the threat and preserving evidence for investigation and legal purposes Recovering and restoring the affected systems and data to a secure state

Evaluating and improving the incident response process and controls based on lessons learned and best practices

Reference = CISM Review Manual, 16th Edition, ISACA, 2021, pages 223-232.

Question: 94

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

A. Documentation of control procedures
B. Standardization of compliance requirements
C. Automation of controls
D. Integration of assurance efforts

Answer: B

Explanation:

= Standardization of compliance requirements is the best approach to reduce unnecessary

duplication of compliance activities, as it allows for a common understanding of the objectives and expectations of various stakeholders, such as regulators, auditors, customers, and business partners. Standardization also facilitates the alignment of compliance activities with the organization's risk appetite and tolerance, and enables the identification and elimination of redundant or conflicting controls. Reference = CISM Review Manual, 27th Edition, page 721; CISM Review Questions, Answers & Explanations Database, 12th Edition, question 952 Learn more:

Question: 95

Which of the following is the GREATEST benefit of conducting an organization-wide security awareness program?

A. The security strategy is promoted.
B. Fewer security incidents are reported.
C. Security behavior is improved.
D. More security incidents are detected.

Answer: C

Explanation:

The greatest benefit of conducting an organization-wide security awareness program is to improve the security behavior of the employees, contractors, partners, and other stakeholders who interact with the organization's information assets. Security behavior refers to the actions and decisions that affect the confidentiality, integrity, and availability of information, such as following the security policies and procedures, reporting security incidents, avoiding risky practices, and applying security controls. By improving the security behavior, the organization can reduce the human-related risks and vulnerabilities, enhance the security culture and awareness, and support the security strategy and objectives.

The other options are not as beneficial as improving the security behavior, although they may also be outcomes or objectives of a security awareness program. Promoting the security strategy is important to communicate the vision, mission, and goals of the security function, as well as to align the security activities

with the business needs and expectations. However, promoting the security strategy alone is not enough to ensure its implementation and effectiveness, as it also requires the involvement and commitment of the stakeholders, especially the senior management. Reporting fewer security incidents may indicate a lower level of security breaches or threats, but it may also reflect a lack of detection, reporting, or awareness mechanisms. Moreover, reporting fewer security incidents is not a reliable measure of the security performance or maturity, as it does not account for the impact, severity, or root causes of the incidents. Detecting more security incidents may indicate a higher level of security monitoring, alerting, or awareness capabilities, but it may also reflect a higher level of security exposures or attacks. Moreover, detecting more security incidents is not a desirable goal of a security awareness program, as it also implies a higher level of security incidents that need to be responded to and resolved. Reference =

CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1006.

The Benefits of Information Security and Privacy Awareness Training Programs, ISACA Journal,

Volume 1, 2019, 1.

Question: 96

An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?

A. Enforce the policy.
B. Modify the policy.
C. Present the risk to senior management.
D. Create an exception for the deviation.

Answer: C

Explanation:

The information security manager’s best course of action is to present the risk to senior management, because this is a case of conflicting objectives and priorities between the information security team and the business management. The information security manager should explain the potential impact and likelihood of a security breach due to the violation of the access policy, as well as the possible legal, regulatory, and reputational consequences. The information security manager should also provide alternative solutions that can achieve both operational efficiency and security compliance, such as implementing single sign-on, role-based access control, or multi-factor authentication. The information security manager should not enforce the policy without senior management’s approval, because this could cause operational disruption and business dissatisfaction. The information security manager should not modify the policy without a proper risk assessment and approval process, because this could weaken the security posture and expose the organization to more threats. The information security manager should not create an exception for the deviation without a formal risk acceptance and documentation process, because this could create inconsistency and ambiguity in the policy enforcement and accountability. Reference = CISM Review Manual, 16th Edition, ISACA, 2021, pages 127-128, 138-139, 143-144.

Question: 97

Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.

Answer: B

Explanation:

= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. Reference =

1: Information Security Incident Response Escalation Guideline2, page 4
2: A Practical Approach to Incident Management Escalation1, section "Step 2: Log the escalation and record the related incident problems that occurred"
3: Computer Security Incident Handling Guide4, page 18

Question: 98

A security incident has been reported within an organization. When should an inforrnation security manager contact the information owner? After the:

A. incident has been confirmed.
B. incident has been contained.
C. potential incident has been logged.
D. incident has been mitigated.

Answer: A

Explanation:

= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.

The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset. Reference = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

Question: 99

Penetration testing is MOST appropriate when a:

A. new system is about to go live.
B. new system is being designed.
C. security policy is being developed.
D. security incident has occurred,

Answer: A

Explanation:

= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process. Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. Reference = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

Question: 100

An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.

Answer: D

Explanation:

= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the postincident review and improvement activities123.

Reference =

1: CISM Review Manual 15th Edition, page 199-2004
2: CISM Practice Quiz, question 1011
3: Computer Security Incident Handling Guide5, page 2-3

Question: 101

Which of the following is the BEST indicator of an organization's information security status?

A. Intrusion detection log analysis
B. Controls audit
C. Threat analysis
D. Penetration test

Answer: B

Explanation:

A controls audit is the best indicator of an organization’s information security status, as it provides an independent and objective assessment of the design, implementation, and effectiveness of the information security controls. A controls audit can also identify the strengths and weaknesses of the information security program, as well as the compliance with the policies, standards, and regulations. A controls audit can cover various aspects of information security, such as governance, risk management, incident management, business continuity, and technical security. A controls audit can be conducted by internal or external auditors, depending on the scope, purpose, and frequency of the audit.

The other options are not as good as a controls audit, as they do not provide a comprehensive and holistic view of the information security status. Intrusion detection log analysis is a technique to monitor and analyze the network or system activities for signs of unauthorized or malicious access or attacks. It can help to detect and respond to security incidents, but it does not measure the overall performance or maturity of the information security program. Threat analysis is a process to identify and evaluate the potential sources, methods, and impacts of threats to the information assets. It can help to prioritize and mitigate the risks, but it does not verify the adequacy or functionality of the

information security controls. Penetration test is a simulated attack on the network or system to evaluate the vulnerability and exploitability of the information security defenses. It can help to validate and improve the technical security, but it does not assess the non-technical aspects of information security, such as governance, policies, or awareness. Reference =
CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1012.

Question: 102

Which of the following is MOST important for building 4 robust information security culture within an organization?

A. Mature information security awareness training across the organization
B. Strict enforcement of employee compliance with organizational security policies
C. Security controls embedded within the development and operation of the IT environment
D. Senior management approval of information security policies

Answer: D

Explanation:

= Mature information security awareness training across the organization is the most important factor for building a robust information security culture, because it helps to educate and motivate the employees to understand and adopt the security policies, procedures, and best practices that are aligned with the organizational goals and values. Information security awareness training should be tailored to the specific roles, responsibilities, and needs of the employees, and should cover the relevant topics, such as:
The importance and value of information assets and the potential risks and threats to them
The legal, regulatory, and contractual obligations and compliance requirements related to information security
The organizational security policies, standards, and guidelines that define the expected and acceptable behaviors and actions regarding information security
The security controls and tools that are implemented to protect the information assets and how to use them effectively and efficiently
The security incidents and breaches that may occur and how to prevent, detect, report, and respond to them
The security best practices and tips that can help to enhance the security posture and culture of the organization
Information security awareness training should be delivered through various methods and channels, such as:
Online courses, webinars, videos, podcasts, and quizzes that are accessible and interactive Classroom sessions, workshops, seminars, and simulations that are engaging and practical Posters, flyers, newsletters, emails, and

social media that are informative and catchy Games, competitions, rewards, and recognition that are fun and incentivizing

Information security awareness training should be conducted regularly and updated frequently, to ensure that the employees are aware of the latest security trends, challenges, and solutions, and that they can demonstrate their knowledge and skills in a consistent and effective manner.

Mature information security awareness training can help to create a positive and proactive security culture that fosters trust, collaboration, and innovation among the employees and the organization, and that supports the achievement of the strategic objectives and the mission and vision of the organization.

Reference = CISM Review Manual, 16th Edition, ISACA, 2021, pages 144-146, 149-150.

Question: 103

The MOST appropriate time to conduct a disaster recovery test would be after:

A. major business processes have been redesigned.
B. the business continuity plan (BCP) has been updated.
C. the security risk profile has been reviewed
D. noncompliance incidents have been filed.

Answer: B

Explanation:

The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well as identify any gaps, issues, or improvement opportunities123. Reference =

1: CISM Review Manual 15th Edition, page 2114
2: CISM Practice Quiz, question 1042
3: Business Continuity Planning and Disaster Recovery Testing, section “Testing the Plan”

Question: 104

Which of the following methods is the BEST way to demonstrate that an information security program provides appropriate coverage?

A. Security risk analysis
B. Gap assessment
C. Maturity assessment
D. Vulnerability scan report

Answer: B

Explanation:

A gap assessment is the best way to demonstrate that an information security program provides appropriate coverage, as it compares the current state of the information security program with the

desired state based on the organization's objectives, policies, standards, and regulations. A gap assessment can identify the strengths and weaknesses of the information security program, as well as the areas that need improvement or alignment. A gap assessment can also provide recommendations and action plans to close the gaps and achieve the desired level of information security coverage.

The other options are not as good as a gap assessment, as they do not provide a comprehensive and holistic view of the information security coverage. Security risk analysis is a process to identify and evaluate the risks to the information assets and the impact of potential threats and vulnerabilities. It can help to prioritize and mitigate the risks, but it does not measure the compliance or performance of the information security program. Maturity assessment is a process to measure the level of maturity of the information security program based on a predefined model or framework. It can help to benchmark and improve the information security program, but it does not account for the specific needs and expectations of the organization. Vulnerability scan report is a document that shows the results of a scan on the network or system to identify the existing or potential vulnerabilities. It can help to validate and improve the technical security, but it does not assess the non-technical aspects of information security, such as governance, policies, or awareness.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1015.

CISM domain 3: Information security program development and management [2022 update], Infosec Certifications, 2.

Question: 105

A recovery point objective (RPO) is required in which of the following?

A. Disaster recovery plan (DRP)
B. Information security plan
C. Incident response plan
D. Business continuity plan (BCP)

Answer: A

Explanation:

A recovery point objective (RPO) is required in a disaster recovery plan (DRP), because it indicates the earliest point in time to which it is acceptable to recover data after a disaster. It effectively quantifies the permissible amount of data loss in case of interruption. It is determined based on the acceptable data loss in case of disruption of operations1. A DRP is a document that defines the procedures, resources, and actions to restore the critical IT systems and data in the event of a disaster that affects the normal operations of the organization2. A DRP should include the RPO for each critical system and data, as well as the backup and restoration methods, frequency, and location to achieve the RPO3.

A RPO is not required in an information security plan, an incident response plan, or a business continuity plan (BCP), because these plans have different purposes and scopes. An information security plan is a document that defines the objectives, policies, standards, and guidelines for information security management in the organization4. An incident response plan is a document that defines the procedures, roles, and responsibilities for identifying, analyzing, responding to, and

learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. A BCP is a document that defines the procedures, resources, and actions to ensure the continuity of the essential business functions and processes in the event of a disruption that affects the normal operations of the organization. These plans may include other metrics, such as recovery time objective (RTO), which is the amount of time after a disaster in which business operation is resumed, or resources are again available for use, but they do not require a RPO. Reference = 1: IS Disaster Recovery Objectives – RunModule 2: Information System Contingency Planning Guidance - ISACA 3: CISM Certified Information Security Manager – Question1411 4: CISM Review Manual, 16th Edition, ISACA, 2021, page 23. : CISM Review Manual, 16th Edition, ISACA, 2021, page 223. : CISM Review Manual, 16th Edition, ISACA, 2021, page 199. : RTO vs. RPO – What is the difference? - Advisera

Question: 106

What should be the FIRST step when an Internet of Things (IoT) device in an organization's network is confirmed to have been hacked?

A. Monitor the network.
B. Perform forensic analysis.
C. Disconnect the device from the network,
D. Escalate to the incident response team

Answer: C

Explanation:

= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network.
Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures123. Reference =

1: CISM Review Manual 15th Edition, page 2004
2: CISM Practice Quiz, question 1072
3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

Question: 107

An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:

A. a control self-assessment (CSA) process.
B. automated reporting to stakeholders.

C. a monitoring process for the security policy.
D. metrics for each milestone.

Answer: D

Explanation:

= Establishing metrics for each milestone is the best way to communicate the program's effectiveness to stakeholders, as it provides a clear and measurable way to track the progress, performance, and outcomes of the information security governance framework. Metrics are quantifiable indicators that can be used to evaluate the achievement of specific objectives, goals, or standards. Metrics can also help to demonstrate the value, benefits, and return on investment of the information security program, as well as to identify and address the gaps, issues, or risks. Metrics for each milestone should be aligned with the organization's strategy, vision, and mission, as well as with the expectations and needs of the stakeholders. Metrics for each milestone should also be SMART (specific, measurable, achievable, relevant, and time-bound), as well as consistent, reliable, and transparent.

The other options are not as important as establishing metrics for each milestone, as they do not provide a comprehensive and holistic way to communicate the program's effectiveness to stakeholders. A control self-assessment (CSA) process is a technique to involve the staff in assessing the design, implementation, and effectiveness of the information security controls. It can help to increase the awareness, ownership, and accountability of the staff, as well as to identify and mitigate the risks. However, a CSA process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not measure the overall performance or maturity of the information security program. Automated reporting to stakeholders is a method to provide timely, accurate, and consistent information to the stakeholders about the status, results, and issues of the information security program. It can help to facilitate the communication, collaboration, and decision making among the stakeholders, as well as to ensure the compliance and transparency of the information security program. However, automated reporting alone is not enough to communicate the program's effectiveness to stakeholders, as it does not evaluate the achievement or impact of the information security program. A monitoring process for the security policy is a process to ensure that the security policy is implemented, enforced, and reviewed in accordance with the organization's objectives, standards, and regulations. It can help to maintain the relevance, adequacy, and effectiveness of the security policy, as well as to incorporate the feedback, changes, and improvements. However, a monitoring process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not cover the other aspects of the information security program, such as governance, risk management, incident management, or business continuity. Reference = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1018.

CISM domain 1: Information security governance [Updated 2022], Infosec, 1.

Key Performance Indicators for Security Governance, Part 1, ISACA Journal, Volume 6, 2020, 2.

Question: 108

Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

A. Collect additional metrics.
B. Perform a cost-benefit analysis.
C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.

Answer: B

Explanation:

The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:

Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements

Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities

Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics

Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process

Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions

A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.

Reference = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

Question: 109

Which of the following BEST enables staff acceptance of information security policies?

A. Strong senior management support
B. Gomputer-based training
C. Arobust incident response program
D. Adequate security funding

Answer: A

Explanation:

= Strong senior management support is the best factor to enable staff acceptance of information security policies, as it demonstrates the commitment and leadership of the organization's top executives in promoting and enforcing a security culture. Senior management support can also help ensure that the information security policies are aligned with the business goals and values, communicated effectively to all levels of the organization, and integrated into the performance evaluation and reward systems. Senior management

support can also help overcome any resistance or challenges from other stakeholders, such as business units, customers, or regulators123. Reference =

1: CISM Review Manual 15th Edition, page 26-274

2: CISM Practice Quiz, question 1102

3: Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, page 5-6

Question: 110

Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?

A. Updated security policies
B. Defined security standards
C. Threat intelligence
D. Regular antivirus updates

Answer: B

Explanation:

Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.

The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.

Advanced Persistent Threats and Nation-State Actors 1
Book Review: Advanced Persistent Threats 2
Advanced Persistent Threat (APT) Protection 3
Establishing Advanced Persistent Security to Combat Long-Term Threats 4
What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

Question: 111

Information security controls should be designed PRIMARILY based on:

A. a business impact analysis (BIA).
B. regulatory requirements.
C. business risk scenarios,
D. a vulnerability assessment.

Answer: C

Explanation:

Information security controls should be designed primarily based on business risk scenarios, because they help to identify and prioritize the most relevant and significant threats and vulnerabilities that may affect the organization's information assets and business objectives. Business risk scenarios are hypothetical situations that describe the possible sources, events, and consequences of a security breach, as well as the likelihood and impact of the occurrence. Business risk scenarios can help to:

Align the information security controls with the business needs and requirements, and ensure that they support the achievement of the strategic goals and the mission and vision of the organization Assess the effectiveness and efficiency of the existing information security controls, and identify the gaps and weaknesses that need to be addressed or improved

Select and implement the appropriate information security controls that can prevent, detect, or mitigate the risks, and that can provide the optimal level of protection and performance for the information assets

Evaluate and measure the return on investment and the value proposition of the information security controls, and communicate and justify the rationale and benefits of the controls to the stakeholders and management

Information security controls should not be designed primarily based on a business impact analysis (BIA), regulatory requirements, or a vulnerability assessment, because these are secondary or complementary factors that influence the design of the controls, but they do not provide the main

basis or criteria for the design. A BIA is a method of estimating and comparing the potential effects of a disruption or a disaster on the critical business functions and processes, in terms of financial, operational, and reputational aspects. A BIA can help to determine the recovery objectives and priorities for the information assets, but it does not identify or address the specific risks and threats that may cause the disruption or the disaster. Regulatory requirements are the legal, contractual, or industry standards and obligations that the organization must comply with regarding information security. Regulatory requirements can help to establish the minimum or baseline level of information security controls that the organization must implement, but they do not reflect the specific or unique needs and challenges of the organization. A vulnerability assessment is a method of identifying and analyzing the weaknesses and flaws in the information systems and assets that may expose them to exploitation or compromise. A vulnerability assessment can help to discover and remediate the

existing or potential security issues, but it does not consider the business context or impact of the issues.

Reference = CISM Review Manual, 16th Edition, ISACA, 2021, pages 119-120, 122-123, 125-126, 129130.

Question: 112

Which of the following is the PRIMARY reason for granting a security exception?

A. The risk is justified by the cost to the business.
B. The risk is justified by the benefit to security.
C. The risk is justified by the cost to security.
D. The risk is justified by the benefit to the business.

Answer: A

Explanation:

= A security exception is a formal authorization to deviate from a security policy, standard, or control, due to a valid business reason or requirement. The primary reason for granting a security exception is that the risk associated with the deviation is justified by the benefit to the business, such as increased efficiency, productivity, customer satisfaction, or competitive advantage. The security exception should be approved by the appropriate authority, such as the senior management or the risk committee, based on a risk assessment and a cost-benefit analysis. The security exception should also be documented, communicated, monitored, and reviewed periodically123. Reference = 1: CISM Review Manual 15th Edition, page 364

2: CISM Practice Quiz, question 1132

3: Security Policy Exception Management, section “Security Policy Exception Management Process”

Question: 113

An organization has acquired a company in a foreign country to gain an advantage in a new market.
Which of the following is the FIRST step the information security manager should take?

A. Determine which country's information security regulations will be used.
B. Merge the two existing information security programs.
C. Apply the existing information security program to the acquired company.
D. Evaluate the information security laws that apply to the acquired company.

Answer: D

Explanation:

The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of the two entities, taking into account the different laws and

regulations, as well as the business objectives and strategies of the acquisition. Reference = : CISM Review Manual 15th Edition, page 32.

Question: 114

An organization's main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?

A. The information security manager
B. The data owner
C. The application owner
D. The security engineer

Answer: C

Explanation:

= The application owner is primarily accountable for the associated task because they are responsible for ensuring that the application meets the business requirements and objectives, as well as the security and compliance standards. The application owner is also the one who defines the roles and responsibilities of the application team, including the security engineer, and oversees the development, testing, deployment, and maintenance of the application. The application owner should work with the cloud provider to address the security vulnerability and mitigate the risk. The information security manager, the data owner, and the security engineer are not primarily accountable for the associated task, although they may have some roles and responsibilities in supporting the application owner. The information security manager is responsible for establishing and maintaining the information security program and aligning it with the business objectives and strategy. The data owner is responsible for defining the classification, usage, and protection requirements of the data. The security engineer is responsible for implementing and testing the security controls and features of the application. Reference = CISM Review Manual 2023, Chapter 1, Section 1.2.2, page 18; CISM Review Questions, Answers & Explanations Database - 12 Month

Subscription, Question ID: 115.

Question: 115

Network isolation techniques are immediately implemented after a security breach to:

A. preserve evidence as required for forensics
B. reduce the extent of further damage.
C. allow time for key stakeholder decision making.
D. enforce zero trust architecture principles.

Answer: B

Explanation:

Network isolation techniques are immediately implemented after a security breach to reduce the extent of further damage by limiting the access and communication of the compromised systems or networks with the rest of the environment. This can help prevent the spread of malware, the exfiltration of data, or the escalation of privileges by the attackers. Network isolation techniques can include disconnecting the affected systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Network isolation techniques are part of the incident response process and should be performed as soon as possible after detecting a security breach. Reference = CISM Review Manual 15th Edition, page 308-3091; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1162

Question: 116

Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?

A. Enable multi-factor authentication on user and admin accounts.
B. Review access permissions annually or whenever job responsibilities change
C. Lock out accounts after a set number of unsuccessful login attempts.
D. Delegate the management of access permissions to an independent third party.

Answer: B

Explanation:

Question: 117

The PRIMARY advantage of involving end users in continuity planning is that they:

A. have a better understanding of specific business needs.
B. are more objective than information security management.
C. can see the overall impact to the business.
D. can balance the technical and business risks.

Answer: A

Explanation:

= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. Reference = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

Question: 118

Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?

A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology

Answer: B

Explanation:

A security awareness program is a set of activities designed to educate and motivate employees to adopt secure behaviors and practices. A security awareness program should be aligned with the organization's business strategy, which defines the vision, mission, goals and objectives of the organization. The most important factor to consider when aligning a security awareness program with the business strategy is the people and culture of the organization, because they are the primary target audience and the key enablers of the program. The people and culture of the organization influence the level of awareness, the attitude and the behavior of the employees towards information security. Therefore, a security awareness program should be tailored to the specific needs, preferences, values and expectations of the people and culture of the organization, and should use appropriate methods, channels, messages and incentives to engage and influence them. A security awareness program that is aligned with the people and culture of the organization will have a higher chance of achieving its objectives and improving the overall security posture of the organization.

Reference =

CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22

Question: 119

IT projects have gone over budget with too many security controls being added post-production.
Which of the following would MOST help to ensure that relevant controls are applied to a project?

A. Involving information security at each stage of project management
B. Identifying responsibilities during the project business case analysis
C. Creating a data classification framework and providing it to stakeholders
D. Providing stakeholders with minimum information security requirements

Answer: A

Explanation:

The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing,

and implementation. This will also help to avoid adding unnecessary or ineffective controls post-production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives. Reference = CISM Review Manual 15th Edition, page 41.

Question: 120

Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?

A. Establish key risk indicators (KRIs).
B. Use quantitative risk assessment methods.
C. Provide regular reporting on risk treatment to senior management
D. Require steering committee approval of risk treatment plans.

Answer: D

Explanation:

= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization's risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business

objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization's risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management. However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. Reference = CISM Review Manual 2023, Chapter 2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

Question: 121

Which of the following would BEST ensure that security is integrated during application development?

A. Employing global security standards during development processes
B. Providing training on secure development practices to programmers

C. Performing application security testing during acceptance testing
D. Introducing security requirements during the initiation phase

Answer: D

Explanation:

Introducing security requirements during the initiation phase would BEST ensure that security is integrated during application development because it would allow the security objectives and controls to be defined and aligned with the business needs and risk appetite before any design or coding is done. This would also facilitate the security by design approach, which is the most effective method to enhance the security of applications and application development activities1. Introducing security requirements early would also enable the collaboration between security professionals and developers, the identification and specification of security architectures, and the integration and testing of security controls throughout the development life cycle2. Employing global security standards during development processes (A) would help to ensure the consistency and quality of security practices, but it would not necessarily ensure that security is integrated during application development. Providing training on secure development practices to programmers (B) would help to raise the awareness and skills of developers, but it would not ensure that security is integrated during application development. Performing application security testing during acceptance testing © would help to verify the security of the application before deployment, but it would not ensure that security is integrated during application development. It would also be too late to identify and remediate any security issues that could have been prevented or mitigated earlier in the

development process. Reference = 1: Five Key Components of an Application Security Program - ISACA1; 2: CISM Domain – Information Security Program Development | Infosec2

Question: 122

Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

A. Internal security audit
B. External security audit
C. Organizational risk appetite
D. Business impact analysis (BIA)

Answer: C

Explanation:

The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. Reference = CISM Review Manual 2023, page 36

Question: 123

Which of the following is the MOST important factor of a successful information security program?

A. The program follows industry best practices.
B. The program is based on a well-developed strategy.
C. The program is cost-efficient and within budget,
D. The program is focused on risk management.

Answer: D

Explanation:

A successful information security program is one that aligns with the business objectives and strategy, supports the business processes and functions, and protects the information assets from threats and vulnerabilities. The most important factor of such a program is that it is focused on risk management, which means that it identifies, assesses, treats, and monitors the information security risks that could affect the business continuity, reputation, and value. Risk management helps to prioritize the security activities and resources, allocate the appropriate budget and resources,

implement the necessary controls and measures, and evaluate the effectiveness and efficiency of the program. Risk management also enables the program to adapt to the changing business and threat environment, and to continuously improve the security posture and performance. A program that follows industry best practices, is based on a well-developed strategy, and is cost-efficient and within budget are all desirable attributes, but they are not sufficient to ensure the success of the program without a risk management focus. Reference = CISM Review Manual 15th Edition, page 411; CISM Practice Quiz, question 1242

Question: 124

Which of the following is the BEST evidence of alignment between corporate and information security governance?

A. Security key performance indicators (KPIs)
B. Project resource optimization
C. Regular security policy reviews
D. Senior management sponsorship

Answer: D

Explanation:

Alignment between corporate and information security governance means that the information security program supports the organizational goals and objectives, and is integrated into the enterprise governance structure. The best evidence of alignment is the senior management sponsorship, which demonstrates the

commitment and support of the top-level executives and board members for the information security program. Senior management sponsorship also ensures that the information security program has adequate resources, authority, and accountability to achieve its objectives and address the risks and issues that affect the organization. Senior management sponsorship also helps to establish a culture of security awareness and compliance throughout the organization, and to communicate the value and benefits of the information security program to the stakeholders.

Reference =

CISM Review Manual 15th Edition, page 1631

CISM 2020: Information Security & Business Process Alignment, video 22

Certified Information Security Manager (CISM), page 33

Question: 125

Which of the following is a desired outcome of information security governance?

A. Penetration test
B. Improved risk management
C. Business agility
D. A maturity model

Answer: C

Explanation:

Business agility is a desired outcome of information security governance, as it enables the organization to respond quickly and effectively to changing business needs and opportunities, while maintaining a high level of security and risk management. Information security governance provides the strategic direction, policies, standards, and oversight for the information security program, ensuring that it aligns with the organization's business objectives and stakeholder expectations. Information security governance also facilitates the integration of security into the business processes and systems, enhancing the organization's ability to adapt to the dynamic and complex environment. By implementing information security governance, the organization can achieve business agility, as well as other benefits such as improved risk management, compliance, reputation, and value creation. Reference = CISM Review Manual 15th Edition, page 25.

Question: 126

Security administration efforts will be greatly reduced following the deployment of which of the following techniques?

A. Discretionary access control
B. Role-based access control
C. Access control lists
D. Distributed access control

Answer: B

Explanation:

Role-based access control (RBAC) is a policy-neutral access control mechanism that assigns access privileges to defined roles in the organization and then makes each user a member of the appropriate roles. RBAC reduces security administration efforts by simplifying the management of access rights across different users and resources. RBAC also enables consistent and efficient enforcement of the principle of least privilege, which grants users only the minimum rights required to perform their assigned tasks. RBAC can also facilitate the implementation of separation of duties, which prevents users from having conflicting or incompatible responsibilities. RBAC is among the most widely used methods in the information security tool kit1. Reference = CIS Control 6: Access Control Management - Netwrix, CISSP certification: RBAC (Role based access control), What is RBAC? (Role Based Access Control) - IONOS

Question: 127

Which of the following is MOST effective in monitoring an organization's existing risk?

A. Periodic updates to risk register

B. Risk management dashboards
C. Security information and event management (SIEM) systems
D. Vulnerability assessment results

Answer: B

Explanation:

Risk management dashboards are the MOST effective in monitoring an organization's existing risk because they provide a visual and interactive representation of the key risk indicators (KRIs) and metrics that reflect the current risk posture and performance of the organization. Risk management dashboards can help to communicate the risk information to various stakeholders, identify trends and patterns, compare actual results with targets and thresholds, and support decision making and risk response12. Periodic updates to risk register (A) are important to maintain the accuracy and relevance of the risk information, but they are not the most effective in monitoring the existing risk because they do not provide a real-time or dynamic view of the risk situation. Security information and event management (SIEM) systems © are effective in monitoring the security events and incidents that may indicate potential or actual threats to the organization, but they are not the most effective in monitoring the existing risk because they do not provide a comprehensive or holistic view of the risk context and impact. Vulnerability assessment results (D) are effective in monitoring the weaknesses and exposures of the organization's assets and systems, but they are not the most effective in monitoring the existing risk because they do not provide a quantitative or qualitative measure of the risk likelihood and consequence. Reference = 1: CISM Review Manual 15th Edition, page 316-3171; 2: CISM Domain 2: Information Risk Management (IRM) [2022 update]2

Question: 128

Which of the following will BEST facilitate the integration of information security governance into enterprise governance?

A. Developing an information security policy based on risk assessments
B. Establishing an information security steering committee

C. Documenting the information security governance framework
D. Implementing an information security awareness program

Answer: B

Explanation:

Establishing an information security steering committee is the best way to facilitate the integration of information security governance into enterprise governance. The information security steering committee is a cross-functional group of senior managers who provide strategic direction, oversight, and support for the information security program. The committee ensures that the information security strategy is aligned with the enterprise strategy, objectives, and risk appetite. The committee also fosters collaboration and communication among various stakeholders and promotes a culture of

security awareness and accountability. Developing an information security policy, documenting the information security governance framework, and implementing an information security awareness program are all important activities for implementing and maintaining information security governance, but they do not necessarily facilitate its integration into enterprise governance. These activities may be initiated or endorsed by the information security steering committee, but they are not sufficient to ensure that information security governance is embedded into the enterprise governance structure and processes. Reference = CISM Review Manual 2023, page 34 1; CISM Practice Quiz 2

Question: 129

Of the following, who is in the BEST position to evaluate business impacts?

A. Senior management
B. Information security manager
C. IT manager
D. Process manager

Answer: D

Explanation:

The process manager is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The process manager has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the process manager is in the best position to evaluate the business impacts of a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The process manager can identify and quantify the potential losses, damages, or consequences that could result from the disruption or incident, such as revenue loss, customer dissatisfaction, regulatory non-compliance, reputational harm, or legal liability. The process manager can also provide input and feedback to the information security manager and the senior management on the business continuity and disaster recovery plans, the risk assessment and treatment, and the security controls and measures that are needed to protect and recover the business processes and functions. Reference = CISM Review Manual 15th Edition, page 2301; CISM Practice Quiz, question

Question: 130

In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOST important for the information security manager to ensure:

A. change activities are documented.
B. the rationale for acceptance is periodically reviewed.
C. the acceptance is aligned with business strategy.
D. compliance with the risk acceptance framework.

Answer: B

Explanation:

= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities, impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management.

Reference =

CISM Review Manual 15th Edition, page 1131

CISM Review Questions, Answers & Explanations Manual 9th Edition, page 482

CISM Domain 2: Information Risk Management (IRM) [2022 update]3

Question: 131

Management decisions concerning information security investments will be MOST effective when they are based on:

A. a process for identifying and analyzing threats and vulnerabilities.
B. an annual loss expectancy (ALE) determined from the history of security events,
C. the reporting of consistent and periodic assessments of risks.
D. the formalized acceptance of risk analysis by management,

Answer: C

Explanation:

Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of

resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. Reference = CISM Review Manual 15th Edition, page 28.

Question: 132

Which of the following service offerings in a typical Infrastructure as a Service (laaS) model will BEST

enable a cloud service provider to assist customers when recovering from a security incident?

A. Availability of web application firewall logs.
B. Capability of online virtual machine analysis
C. Availability of current infrastructure documentation
D. Capability to take a snapshot of virtual machines

Answer: D

Explanation:

A snapshot is a point-in-time copy of the state of a virtual machine (VM) that can be used to restore the VM to a previous state in case of a security incident or a disaster. A snapshot can capture the VM's disk, memory, and device configuration, allowing for a quick and easy recovery of the VM's data and functionality. Snapshots can also be used to create backups, clones, or replicas of VMs for testing, analysis, or migration purposes. Snapshots are a common service offering in Infrastructure as a Service (IaaS) models, where customers can provision and manage VMs on demand from a cloud service provider (CSP). A CSP that offers the capability to take snapshots of VMs can assist customers when recovering from a security incident by providing them with the following benefits12:

Faster recovery time: Snapshots can reduce the downtime and data loss caused by a security incident by allowing customers to quickly revert their VMs to a known good state. Snapshots can also help customers avoid the need to reinstall or reconfigure their VMs after an incident, saving time and resources.

Easier incident analysis: Snapshots can enable customers to perform online or ofline analysis of their VMs after an incident, without affecting the production environment. Customers can use snapshots to examine the VM's disk, memory, and logs for evidence of compromise, root cause analysis, or forensic investigation. Customers can also use snapshots to test and validate their incident response plans or remediation actions before applying them to the production VMs.

Enhanced security posture: Snapshots can improve the security posture of customers by enabling them to implement best practices such as backup and restore, disaster recovery, and business continuity. Snapshots can help customers protect their VMs from accidental or malicious deletion, corruption, or modification, as well as from environmental or technical disruptions. Snapshots can also help customers comply with regulatory or contractual requirements for data retention, availability, or integrity. Reference = What is Disaster Recovery as a Service? | CSA - Cloud Security Alliance, What Is Cloud Incident Response (IR)? CrowdStrike

Question: 133

When developing an asset classification program, which of the following steps should be completed FIRST?

A. Categorize each asset.
B. Create an inventory. &
C. Create a business case for a digital rights management tool.
D. Implement a data loss prevention (OLP) system.

Answer: B

Explanation:

Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified. An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification12. Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset12. Creating a business case for a digital rights management tool © is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets3. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media4. Reference = 1: CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA2; 3: What is Digital Rights Management? - Definition from Techopedia3; 4: What is Data Loss Prevention (DLP)? - Definition from Techopedia4

Question: 134

A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information security manager's BEST course of action?

A. Instruct the vendor to conduct penetration testing.
B. Suspend the connection to the application in the firewall
C. Report the situation to the business owner of the application.
D. Initiate the organization's incident response process.

Answer: D

Explanation:

= Initiating the organization’s incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability. The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant

stakeholders. The incident response process

should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application. Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action. Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application. Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. Reference = CISM Review Manual 2023, page 211 1; CISM Practice Quiz 2

Question: 135

Which of the following BEST facilitates effective incident response testing?

A. Including all business units in testing
B. Simulating realistic test scenarios
C. Reviewing test results quarterly
D. Testing after major business changes

Answer: B

Explanation:

Effective incident response testing is a process of verifying and validating the incident response plan, procedures, roles, and resources that are designed to respond to and recover from information security incidents. The purpose of testing is to ensure that the incident response team and the organization are prepared, capable, and confident to handle any potential or actual incidents that could affect the business continuity, reputation, and value. The best way to facilitate effective testing is to simulate realistic test scenarios that reflect the most likely or critical threats and vulnerabilities that could cause an incident, and the most relevant or significant impacts and consequences that could result from an incident. Simulating realistic test scenarios can help to evaluate the adequacy, accuracy, and applicability of the incident response plan, procedures, roles, and resources, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the incident response process. Simulating realistic test scenarios can also help to enhance the skills, knowledge, and experience of the incident response team and the organization, as well as to improve the communication, coordination, and collaboration among the stakeholders involved in the incident response process. Simulating realistic test scenarios can also help to measure and report the effectiveness and efficiency of the incident response process, and to provide feedback and recommendations for improvement and optimization. Reference = CISM Review Manual 15th Edition, page 2401; CISM Practice Quiz, question 1362

Question: 136

An organization needs to comply with new security incident response requirements. Which of the following should the information security manager do FIRST?

A. Create a business case for a new incident response plan.
B. Revise the existing incident response plan.
C. Conduct a gap analysis.
D. Assess the impact to the budget,

Answer: C

Explanation:

Before implementing any changes to the security incident response plan, the information security manager should first conduct a gap analysis to identify the current state of the plan and compare it with the new requirements. A gap analysis is a systematic process of evaluating the differences between the current and desired state of a system, process, or program. A gap analysis can help to identify the strengths and weaknesses of the existing plan, the gaps that need to be addressed, the priorities and dependencies of the actions, and the resources and costs involved. A gap analysis can also help to create a business case for the changes and justify the investment. A gap analysis can be conducted using various methods and tools, such as frameworks, standards, benchmarks, questionnaires, interviews, audits, or tests1234.

Reference =
CISM Review Manual 15th Edition, page 1631
CISM certified information security manager study guide, page 452
How To Conduct An Information Security Gap Analysis3
PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS4

Question: 137

Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

A. Security policy
B. Risk management framework
C. Risk appetite
D. Security standards

Answer: C

Explanation:

= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well

as the selection and implementation of security controls. Risk appetite must be defined in order for an

information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. Reference = CISM Review Manual 15th Edition, page 29, page 31.

Question: 138

When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

A. best practices.
B. control framework
C. regulatory requirements.
D. cost-benefit analysis,

Answer: D

Explanation:

Cost-benefit analysis (CBA) is a method of comparing the costs and benefits of different alternatives for achieving a desired outcome. CBA can help information security managers to choose the best controls to mitigate risk to acceptable levels by providing a rational and objective basis for decision making. CBA can also help information security managers to justify their choices to senior management, stakeholders, and auditors by demonstrating the value and return on investment of the selected controls. CBA can also help information security managers to prioritize and allocate resources for implementing and maintaining the controls12.

CBA involves the following steps12:

Identify the objectives and scope of the analysis

Identify the alternatives and options for achieving the objectives

Identify and quantify the costs and benefits of each alternative

Compare the costs and benefits of each alternative using a common metric or criteria Select the alternative that maximizes the net benefit or minimizes the net cost Perform a sensitivity analysis to test the robustness and validity of the results Document and communicate the results and recommendations

CBA is mainly driven by the information security manager’s decision, but it can also take into account other factors such as best practices, control frameworks, and regulatory requirements. However, these factors are not the primary drivers of CBA, as they may not always reflect the specific needs and context of the organization. Best practices are general guidelines or recommendations that may not suit every situation or environment. Control frameworks are standardized models or methodologies that may not cover all aspects or dimensions of information security. Regulatory requirements are mandatory rules or obligations that may not address all risks or threats faced by the organization. Therefore, CBA is the best method to choose the most appropriate and effective controls to mitigate risk to acceptable levels, as it considers the costs and benefits of each control in relation to the organization’s objectives, resources, and environment12. Reference = CISM Domain 2: Information Risk Management (IRM) [2022 update], Five Key Considerations When Developing Information Security Risk Treatment Plans

Question: 139

Which of the following MUST happen immediately following the identification of a malware incident?

A. Preparation
B. Recovery
C. Containment
D. Eradication

Answer: C

Explanation:

Containment is the action that MUST happen immediately following the identification of a malware incident because it aims to isolate the affected systems or networks from the rest of the environment and prevent the spread or escalation of the malware. Containment can involve disconnecting the systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Containment is part of the incident response process and should be performed as soon as possible after detecting a malware incident12. Preparation (A) is the phase that happens before the identification of a malware incident, where the organization establishes the incident response plan, team, roles, resources, and tools. Preparation is essential for ensuring the readiness and capability of the organization to respond to malware incidents effectively and efficiently12. Recovery (B) is the phase that happens after the containment and eradication of a malware incident, where the organization restores the normal operations of the systems or networks, verifies the functionality and security of the systems or networks, and implements the preventive and corrective measures to avoid or mitigate future malware incidents. Recovery is the final phase of the incident response process and should be performed after ensuring that the malware incident is fully resolved and the systems or networks are clean and secure12. Eradication (D) is the phase that happens after the containment of a malware incident, where the organization removes the malware and its traces from the systems or networks, identifies the root cause and impact of the malware incident, and collects and preserves the evidence for analysis and investigation. Eradication is an important phase of the incident response process, but it does not happen immediately after the identification of a malware incident12.
Reference = 1: CISM Review Manual 15th Edition, page 308-3091; 2: Cybersecurity Incident Response Exercise Guidance - ISACA2

Question: 140

Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?

A. Compromise of critical assets via third-party resources
B. Unavailability of services provided by a supplier
C. Loss of customers due to unavailability of products
D. Unreliable delivery of hardware and software resources by a supplier

Answer: A

Explanation:

= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness. Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios. These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. Reference = CISM Review Manual 2023, page 189 1; CISM Practice Quiz 2

Question: 141

An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. conduct an incident forensic analysis.
B. fallow the incident response plan
C. notify the business process owner.
D. fallow the business continuity plan (BCP).

Answer: B

Explanation:

Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified as a security incident that requires further escalation, investigation, and resolution. Following the incident

response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.

Conducting an incident forensic analysis, notifying the business process owner, and following the business

continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident.
Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been identified and implemented. Reference = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

Question: 142

A PRIMARY purpose of creating security policies is to:

A. define allowable security boundaries.
B. communicate management's security expectations.
C. establish the way security tasks should be executed.
D. implement management's security governance strategy.

Answer: D

Explanation:

A security policy is a formal statement of the rules and principles that govern the protection of information assets in an organization. A security policy defines the scope, objectives, roles and responsibilities, and standards of the information security program. A primary purpose of creating security policies is to implement management's security governance strategy, which is the framework that guides the direction and alignment of information security with the business goals and objectives. A security policy translates the management's vision and expectations into specific and measurable requirements and controls that can be implemented and enforced by the information security staff and other stakeholders. A security policy also helps to establish the accountability and authority of the information security function and to demonstrate the commitment and support of the senior management for the information security program. Reference =
CISM Review Manual 15th Edition, page 1631
CISM 2020: IT Security Policies2
CISM domain 1: Information security governance [Updated 2022]3
What is CISM? - Digital Guardian4

Question: 143

Which of the following BEST supports information security management in the event of organizational changes in security personnel?

A. Formalizing a security strategy and program
B. Developing an awareness program for staff
C. Ensuring current documentation of security processes
D. Establishing processes within the security operations team

Answer: C

Explanation:

Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational changes in security personnel, and ensure a smooth transition and alignment of the security program. Reference = CISM Review Manual 15th Edition, page 43, page 45.

Question: 144

Which of the following is the PRIMARY reason to monitor key risk indicators (KRIs) related to information security?

A. To alert on unacceptable risk
B. To identify residual risk
C. To reassess risk appetite
D. To benchmark control performance

Answer: A

Explanation:

Key risk indicators (KRIs) are metrics that measure the level of risk exposure and the likelihood of occurrence of potential adverse events that can affect the organization's objectives and performance. KRIs are used to monitor changes in the risk environment and to provide early warning signals for potential issues that may require management attention or intervention. KRIs are also used to communicate the risk status and trends to the relevant stakeholders and to support riskbased decision making12.

The primary reason to monitor KRIs related to information security is to alert on unacceptable risk. Unacceptable risk is the level of risk that exceeds the organization's risk appetite, tolerance, or threshold, and that poses a significant threat to the organization's assets, operations, reputation, or compliance. Unacceptable risk can result from internal or external factors, such as cyberattacks, data breaches, system failures, human errors, fraud, natural disasters, or regulatory changes. Unacceptable risk can have severe consequences for the organization, such as financial losses, legal liabilities, operational disruptions, customer dissatisfaction, or reputational damage12. By monitoring KRIs related to information security, the organization can identify and assess the sources, causes, and impacts of unacceptable risk, and take timely and appropriate actions to mitigate, transfer, avoid, or accept the risk. Monitoring KRIs can also help the organization to evaluate the effectiveness and efficiency of the existing information security controls, policies, and procedures, and to identify and implement any necessary improvements or enhancements. Monitoring KRIs can also help the organization to align its information security strategy and objectives with its business strategy and

objectives, and to ensure compliance with the relevant laws, regulations, standards, and best practices12.

While monitoring KRIs related to information security can also serve other purposes, such as identifying residual risk, reassessing risk appetite, or benchmarking control performance, these are not the primary reason for monitoring KRIs. Residual risk is the level of risk that remains after applying the risk treatment options, and it should be within the organization's risk appetite, tolerance, or threshold. Reassessing risk appetite is the process of reviewing and adjusting the amount and type of risk that the organization is willing to take in pursuit of its objectives, and it should be done periodically or when there are significant changes in the internal or external environment. Benchmarking control performance is the process of comparing the organization's information security controls with those of other organizations or industry standards, and it should be done to identify and adopt the best practices or to demonstrate compliance12. Reference = Integrating KRIs and KPIs for Effective Technology Risk Management, The Power of KRIs in Enterprise Risk Management (ERM) - Metricstream, What Is a Key Risk Indicator? With Characteristics and Tips, KRI Framework for Operational Risk Management | Workiva, Key risk indicator - Wikipedia

Question: 145

If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:

A. contact law enforcement.
B. document the chain of custody.
C. capture evidence using standard server-backup utilities.
D. reboot affected machines in a secure area to search for evidence.

Answer: B

Explanation:

Documenting the chain of custody is the PRIMARY step for an organizational response to a security incident if civil litigation is a goal because it ensures the integrity, authenticity, and admissibility of the evidence collected from the incident. The chain of custody is the process of documenting the

history of the evidence, including its identification, collection, preservation, transportation, analysis, storage, and presentation in court. The chain of custody should include information such as the date, time, location, description, source, owner, handler, and purpose of each evidence item, as well as any changes, modifications, or transfers that occurred to the evidence. Documenting the chain of custody can help to prevent the evidence from being tampered with, altered, lost, or destroyed, and to demonstrate that the evidence is relevant, reliable, and original12. Contacting law enforcement (A) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a possible or optional step depending on the nature, severity, and jurisdiction of the incident. Contacting law enforcement may help to obtain legal assistance, guidance, or support, but it may also involve risks such as loss of control, confidentiality, or reputation. Therefore, contacting law enforcement should be done after careful consideration of the legal obligations, contractual agreements, and organizational policies12. Capturing evidence using standard server-backup utilities © is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Capturing evidence using standard server-backup utilities may help to preserve the state of the systems or networks

involved in the incident, but it may also introduce changes or errors that could compromise the validity or quality of the evidence. Therefore, capturing evidence using standard server-backup utilities should be done using forensically sound methods and tools, and following the documented chain of custody12. Rebooting affected machines in a secure area to search for evidence (D) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Rebooting affected machines in a secure area may help to isolate and analyze the systems or networks involved in the incident, but it may also cause the loss or alteration of the evidence, such as volatile memory, temporary files, or logs. Therefore, rebooting affected machines in a secure area should be done with caution and following the documented chain of custody12. Reference = 1: CISM Review Manual 15th Edition, page 310-3111; 2: CISM Domain 4: Information Security Incident Management (ISIM) [2022 update]2

Question: 146

Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?

A. Develop the test plan.
B. Analyze the business impact.
C. Define response team roles.
D. Identify recovery time objectives (RTOs).

Answer: A

Explanation:

= Developing the test plan is the task that should be performed once a disaster recovery plan (DRP) has been developed. The test plan is a document that describes the objectives, scope, methods, and procedures for testing the DRP. The test plan should also define the roles and responsibilities of the test team, the test scenarios and criteria, the test schedule and resources, and the test reporting and evaluation. The purpose of testing the DRP is to verify its effectiveness, identify any gaps or

weaknesses, and improve its reliability and usability. Testing the DRP also helps to increase the awareness and readiness of the staff and stakeholders involved in the disaster recovery process. Analyzing the business impact, defining response team roles, and identifying recovery time objectives (RTOs) are all tasks that should be performed before developing the DRP, not after. These tasks are part of the business continuity planning (BCP) process, which aims to identify the critical business functions and assets, assess the potential threats and impacts, and determine the recovery strategies and requirements. The DRP is a subset of the BCP that focuses on restoring the IT systems and services after a disaster. Therefore, the DRP should be based on the results of the BCP process, and tested after it has been developed. Reference = CISM Review Manual 2023, page 218 1; CISM Practice Quiz 2

Question: 147

In violation of a policy prohibiting the use of cameras at the office, employees have been issued smartphones and tablet computers with enabled web cameras. Which of the following should be the information security manager's FIRST course of action?

A. Revise the policy.
B. Perform a root cause analysis.
C. Conduct a risk assessment,
D. Communicate the acceptable use policy.

Answer: C

Explanation:

= The information security manager's first course of action in this situation should be to conduct a risk assessment, which is a process of identifying, analyzing, and evaluating the information security risks that arise from the violation of the policy prohibiting the use of cameras at the office. The risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate use of the cameras on the smartphones and tablet computers, such as capturing, transmitting, or disclosing sensitive or confidential information, compromising the privacy or security of the employees, customers, or partners, or violating the legal or regulatory requirements. The risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to disable, restrict, or monitor the camera usage, enforcing the policy compliance and awareness, or revising the policy to reflect the current business needs and environment. The risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the policy and the risk management process. Revising the policy, performing a root cause analysis, and communicating the acceptable use policy are all possible courses of action that the information security manager can take after conducting the risk assessment, but they are not the first ones. Revising the policy is a process of updating and modifying the policy to align with the business objectives and strategy, to address the changes and challenges in the business and threat environment, and to incorporate the feedback and suggestions from the risk assessment and the stakeholders. Performing a root cause analysis is a process of investigating and identifying the underlying causes and factors that led to the violation of the policy,

such as the lack of awareness, training, or enforcement, the inconsistency or ambiguity of the policy, or the conflict or gap between the policy and the business requirements or expectations. Communicating the acceptable use policy is a process of informing and educating the employees and the other users of the smartphones and tablet computers about the purpose, scope, and content of the policy, the roles and responsibilities of the users, the benefits and consequences of complying or violating the policy, and the methods and channels of reporting or resolving any policy issues or incidents. Reference = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1482

Question: 148

Which of the following is an information security manager's MOST important course of action when responding to a major security incident that could disrupt the business?

A. Follow the escalation process.
B. Identify the indicators of compromise.
C. Notify law enforcement.
D. Contact forensic investigators.

Answer: A

Explanation:

When responding to a major security incident that could disrupt the business, the information security manager's most important course of action is to follow the escalation process. The escalation process is a predefined set of steps and procedures that define who should be notified, when, how, and with what information in the event of a security incident. The escalation process helps to ensure that the appropriate stakeholders, such as senior management, business units, legal counsel, public relations, and external parties, are informed and involved in the incident response process. The escalation process also helps to coordinate the actions and decisions of the incident response team and the business continuity team, and to align the incident response objectives with the business priorities and goals. The escalation process should be documented and communicated as part of the incident response plan, and should be reviewed and updated regularly to reflect the changes in the organization's structure, roles, and responsibilities.

Reference =

CISM Review Manual 15th Edition, page 1631

CISM 2020: Incident Management and Response, video 32

Incident Response Models3

Question: 149

Which of the following would be MOST helpful to identify worst-case disruption scenarios?

A. Business impact analysis (BIA)
B. Business process analysis
C. SWOT analysis
D. Cast-benefit analysis

Answer: A

Explanation:

A business impact analysis (BIA) is the process of identifying and evaluating the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization in the event of a disaster or crisis. A BIA also helps to identify the worst-case disruption scenarios, which are the scenarios that would cause the most severe impact to the organization in terms of financial, operational, reputational, or legal consequences. By conducting a BIA, the organization can assess the likelihood and impact of various disruption scenarios, and plan accordingly to mitigate the risks and ensure business continuity and resilience. Reference = CISM Review Manual 15th Edition, page 181, page 183.

Question: 150

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

A. results of exit interviews.
B. previous training sessions.
C. examples of help desk requests.
D. responses to security questionnaires.

Answer: C

Explanation:

The best way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include examples of help desk requests. Help desk requests are requests for assistance or support from users who encounter problems or issues related to information security, such as password resets, malware infections, phishing emails, unauthorized access, data loss, or system errors. Help desk requests can provide valuable insights into the types, frequencies, and impacts of the incidents that affect the users, as well as the users' knowledge, skills, and behaviors regarding information security. By including examples of help desk requests in the user security awareness training program, the information security manager can achieve the following benefits12:

Increase the relevance and effectiveness of the training content: By using real-life scenarios and cases that the users have experienced or witnessed, the information security manager can make the training content more relevant, engaging, and applicable to the users' needs and situations. The information security manager can also use the examples of help desk requests to illustrate the consequences and costs of the incidents, and to highlight the best practices and solutions to prevent or resolve them. This can help the users to understand the importance and value of information security, and to improve their knowledge, skills, and attitudes accordingly.

Identify and address the gaps and weaknesses in the training program: By analyzing the patterns and trends of the help desk requests, the information security manager can identify and address the gaps and weaknesses in the existing training program, such as outdated or inaccurate information, insufficient or ineffective coverage of topics, or lack of feedback or evaluation. The information security manager can also use the examples of help desk requests to measure and monitor the impact and outcomes of the training program, such as changes in the number, type, or severity of the incidents, or changes in the users' satisfaction, performance, or behavior.

Enhance the communication and collaboration with the users and the help desk staff: By including examples of help desk requests in the user security awareness training program, the information security manager can enhance the communication and collaboration with the users and the help desk staff, who are the key stakeholders and partners in information security. The information security manager can use the examples of help desk requests to solicit feedback, suggestions, or questions from the users and the help desk staff, and to provide them with timely and relevant information, guidance, or support. The information security manager can also use the examples of help desk requests to recognize and appreciate the efforts and contributions of the users and the help desk staff in reporting, responding, or resolving the incidents, and to encourage and motivate them to continue their involvement and participation in information security.

The other options are not the best way to ensure that frequently encountered incidents are reflected in the user security awareness training program, as they are less reliable, relevant, or effective sources of information. Results of exit interviews are feedback from employees who are leaving the organization, and they may not reflect the current or future incidents that the remaining or new employees may face. Previous training sessions are records of the past training activities, and they may not capture the changes or updates in the information security environment, threats, or requirements. Responses to security questionnaires are answers to predefined questions or surveys, and they may not cover all the possible or emerging incidents that the users may encounter or experience12. Reference = Information Security Awareness Training: Best Practices

- Infosec Resources, How to Create an Effective Security Awareness Training Program - Infosec Resources, Security Awareness Training: How to Build a Successful Program - ISACA, Security Awareness Training: How to Educate Your Employees - ISACA

Question: 151

Which of the following is MOST helpful for aligning security operations with the IT governance framework?

A. Security risk assessment
B. Security operations program
C. Information security policy
D. Business impact analysis (BIA)

Answer: C

Explanation:

An information security policy is the MOST helpful for aligning security operations with the IT governance framework because it defines the security objectives, principles, standards, and guidelines that guide the security operations activities and processes. An information security policy

also establishes the roles and responsibilities, authorities and accountabilities, and reporting and communication mechanisms for security operations. An information security policy should be aligned with the IT governance framework, which provides the direction, structure, and oversight for the effective management and delivery of IT services and resources. An information security policy should also be consistent with the enterprise governance framework, which sets the vision, mission, values, and goals of the organization12. A security risk assessment (A) is helpful for identifying and evaluating the security risks that may affect the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A security risk assessment should be based on the information security policy, which defines the risk appetite, tolerance, and criteria for the organization12. A security operations program (B) is helpful for implementing and executing the security operations activities and processes that support the IT governance framework, but it is not the MOST helpful for aligning them. A security operations program should be derived from the information security policy, which provides the strategic direction and guidance for the security operations12. A business impact analysis (BIA) (D) is helpful for determining the criticality and priority of the business processes and functions that depend on the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A BIA should be conducted in accordance with the information security policy, which specifies the business continuity and disaster recovery requirements and objectives for the organization12. Reference = 1: CISM Review Manual 15th Edition, page 75-76, 81-82, 88-89, 93-941; 2: CISM Domain 1: Information Security Governance (ISG) [2022 update]2

Question: 152

Which of the following desired outcomes BEST supports a decision to invest in a new security initiative?

A. Enhanced security monitoring and reporting
B. Reduced control complexity
C. Enhanced threat detection capability

D. Reduction of organizational risk

Answer: D

Explanation:

The reduction of organizational risk is the desired outcome that best supports a decision to invest in a new security initiative. The organizational risk is the level of exposure or uncertainty that the organization faces in achieving its objectives. The organizational risk is influenced by various factors, such as the threat landscape, the vulnerability of the assets, the impact of the incidents, and the effectiveness of the controls. The information security manager should evaluate the organizational risk and propose security initiatives that can reduce the risk to an acceptable level. The security initiatives should be aligned with the business goals, the risk appetite, and the available resources of the organization. The security initiatives should also provide a positive return on investment (ROI) or value for money (VFM) for the organization. The reduction of organizational risk is the ultimate goal and benefit of any security initiative, as it enhances the security posture, performance, and resilience of the organization. Enhanced security monitoring and reporting, reduced control complexity, and enhanced threat detection capability are all possible outcomes of security initiatives, but they are

not the best ones to support a decision to invest in a new security initiative. These outcomes are more specific and technical, and they may not directly relate to the business objectives or the risk appetite of the organization. These outcomes are also intermediate or enabling, rather than final or ultimate, as they may not necessarily lead to the reduction of organizational risk. For example, enhanced security monitoring and reporting may improve the visibility and awareness of the security status, but it may not prevent or mitigate the incidents. Reduced control complexity may simplify the security management and maintenance, but it may not address the emerging or evolving threats. Enhanced threat detection capability may increase the speed and accuracy of identifying the attacks, but it may not reduce the impact or the likelihood of the attacks. Therefore, the reduction of organizational risk is the best outcome to support a decision to invest in a new security initiative, as it demonstrates the value and effectiveness of the security initiative for the organization.
Reference = CISM Review Manual 2023, page 40 1; CISM Practice Quiz 2

Question: 153

A Seat a-hosting organization's data center houses servers, appli
BEST approach for developing a physical access control policy for the organization?

A. Review customers' security policies.
B. Conduct a risk assessment to determine security risks and mitigating controls.
C. Develop access control requirements for each system and application.
D. Design single sign-on (SSO) or federated access.

Answer: B

Explanation:

= The best approach for developing a physical access control policy for the organization is to conduct a risk assessment to determine the security risks and mitigating controls that are relevant and appropriate for the organization's data center. A risk assessment is a process of identifying, analyzing, and evaluating the

information security risks that could affect the availability, integrity, or confidentiality of the servers, applications, and data that are hosted in the data center. A risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate physical access to the data center, such as theft, damage, sabotage, or espionage, and the potential consequences for the organization and its customers, such as service disruption, data loss, data breach, or legal liability. A risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to prevent, detect, or respond to the physical access incidents, such as locks, alarms, cameras, guards, badges, or logs. A risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the physical access control policy and the risk management process.
Reviewing customers' security policies, developing access control requirements for each system and application, and designing single sign-on (SSO) or federated access are all possible steps that the organization can take after conducting the risk assessment, but they are not the best ones. Reviewing customers' security policies is a process of understanding and complying with the customers' expectations and requirements for the security of their servers, applications, and data that are

hosted in the data center, and ensuring that the organization's physical access control policy is consistent and compatible with them. Developing access control requirements for each system and application is a process of defining and implementing the specific rules and criteria for granting or denying the physical access to the servers and applications that are hosted in the data center, based on the roles, responsibilities, and privileges of the users, and the sensitivity and criticality of the systems and applications. Designing single sign-on (SSO) or federated access is a process of enabling and facilitating the authentication and authorization of the users who need to access the servers and applications that are hosted in the data center, by using a single or shared identity and credential across multiple systems and domains. Reference = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1542

Question: 154

Which of the following would BEST help to ensure appropriate security controls are built into software?

A. Integrating security throughout the development process
B. Performing security testing prior to deployment
C. Providing standards for implementation during development activities
D. Providing security training to the software development team

Answer: A

Explanation:

The best way to ensure appropriate security controls are built into software is to integrate security throughout the development process. This means that security should be considered from the initial stages of planning, design, coding, testing, deployment, and maintenance of the software.
Integrating security throughout the development process helps to identify and mitigate security risks early, reduce the cost and complexity of fixing vulnerabilities later, improve the quality and reliability of the software, and enhance the trust and confidence of the users and customers. Integrating security throughout the development process also aligns with the best practices and standards of information security governance, such as the CISM framework123.
Reference =

CISM Review Manual 15th Edition, page 1631
CISM domain 3: Information security program development and management [2022 update]2
CISSP domain 8 overview: Software development security4

Question: 155

Which of the following will ensure confidentiality of content when accessing an email system over the Internet?

A. Multi-factor authentication
B. Digital encryption
C. Data masking
D. Digital signatures

Answer: B

Explanation:

Digital encryption is the process of transforming data into an unreadable form using a secret key or algorithm. Digital encryption will ensure the confidentiality of content when accessing an email system over the Internet, as it prevents unauthorized parties from intercepting, viewing, or modifying the email messages. Digital encryption can be applied to both the email content and the email transmission, using different methods such as symmetric encryption, asymmetric encryption, or hybrid encryption. Digital encryption can also provide other benefits such as authentication, integrity, and non-repudiation, depending on the encryption scheme and the use of digital signatures or certificates. Reference = CISM Review Manual 15th Edition, page 101, page 102.

Question: 156

What should be an information security manager's MOST important consideration when developing a multi-year plan?

A. Ensuring contingency plans are in place for potential information security risks
B. Ensuring alignment with the plans of other business units
C. Allowing the information security program to expand its capabilities
D. Demonstrating projected budget increases year after year

Answer: B

Explanation:

= The most important consideration when developing a multi-year plan for information security is to ensure alignment with the plans of other business units. Alignment means that the information security plan supports and enables the achievement of the business objectives, strategies, and priorities of the organization and its various units. Alignment also means that the information security plan is consistent and compatible with the

plans of other business units, and that it addresses the needs, expectations, and requirements of the relevant stakeholders1 .

By ensuring alignment with the plans of other business units, the information security manager can achieve the following benefits1 :

Increase the value and effectiveness of information security: By aligning the information security plan with the business goals and drivers, the information security manager can demonstrate the value and contribution of information security to the organization's performance, growth, and competitiveness. The information security manager can also ensure that the information security plan addresses the most critical and relevant risks and opportunities for the organization and its units, and that it provides adequate and appropriate protection and support for the organization's assets, processes, and activities.

Enhance the communication and collaboration with other business units: By aligning the information security plan with the plans of other business units, the information security manager can enhance the communication and collaboration with the other business unit leaders and managers, who are the key stakeholders and partners in information security. The information security manager can also solicit and incorporate their input, feedback, and suggestions into the information security plan, and provide them with timely and relevant information, guidance, and support. The information security manager can also foster a culture of trust, respect, and cooperation among the different business units, and promote a shared vision and commitment to information security.

Optimize the use and allocation of resources for information security: By aligning the information security plan with the plans of other business units, the information security manager can optimize the use and allocation of resources for information security, such as budget, staff, time, or technology. The information security manager can also avoid duplication, conflict, or waste of resources among the different business units, and ensure that the information security plan is feasible, realistic, and sustainable. The information security manager can also leverage the resources and capabilities of other business units to enhance the information security plan, and provide them with the necessary resources and capabilities to implement and maintain the information security plan.

The other options are not the most important consideration when developing a multi-year plan for information security, as they are less strategic, comprehensive, or impactful than ensuring alignment with the plans of other business units. Ensuring contingency plans are in place for potential information security risks is an important component of the information security plan, but it is not the most important consideration, as it focuses on the reactive and preventive aspects of information security, rather than the proactive and enabling aspects. Allowing the information security program to expand its capabilities is an important objective of the information security plan, but it is not the most important consideration, as it depends on the availability and suitability of the resources, technologies, and opportunities for information security, and it may not align with the organization's needs, priorities, or constraints. Demonstrating projected budget increases year after year is an important outcome of the information security plan, but it is not the most important consideration, as it reflects the cost and demand of information security, rather than the value and benefit of information security, and it may not be justified or supported by the organization's financial situation or expectations1 . Reference = CISM Domain 1: Information Security Governance (ISG) [2022 update], CISM Domain 2: Information Risk Management (IRM) [2022 update], Aligning Information Security with Business Strategy - ISACA, [Aligning Information Security with Business Objectives - ISACA]

Question: 157

An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?

A. Review independent security assessment reports for each vendor.

B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.

Answer: D

Explanation:

Defining information security requirements and processes is the FIRST thing that the information security manager should do to support the initiative of utilizing Software as a Service (SaaS) and selecting a vendor. This is because information security requirements and processes provide the basis for evaluating and comparing the SaaS vendors and solutions, as well as for ensuring the alignment of the SaaS services with the organization's security objectives, policies, and standards. Information security requirements and processes should include aspects such as data protection, access control, encryption, authentication, authorization, audit, compliance, incident response, disaster recovery, and service level agreements12. Reviewing independent security assessment reports for each vendor (A) is a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Independent security assessment reports can provide valuable information about the security posture, practices, and performance of the SaaS vendors and solutions, such as their compliance with industry standards, frameworks, and regulations, their vulnerability and risk management, and their security testing and auditing results. However, reviewing independent security assessment reports should be done after defining the information security requirements and processes, which can help to determine the scope, criteria, and expectations for the security assessment12. Benchmarking each vendor's services with industry best practices (B) is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Benchmarking each vendor's services with industry best practices can help to measure and compare the quality, performance, and value of the SaaS vendors and solutions, as well as to identify the gaps, strengths, and weaknesses of the SaaS services. However, benchmarking each vendor's services with industry best practices should be done after defining the information security requirements and processes, which can help to select the relevant and appropriate industry best practices for the SaaS services12. Analyzing the risks and proposing mitigating controls © is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Analyzing the risks and proposing mitigating controls can help to identify and evaluate the potential threats, vulnerabilities, and impacts that may affect the security, availability, and reliability of the SaaS vendors and solutions, as well as to recommend and implement the necessary measures to reduce or eliminate the risks. However, analyzing the risks and proposing mitigating controls should be done after defining the information security requirements and processes, which can help to establish the risk appetite, tolerance, and criteria for the SaaS services12. Reference = 1: CISM Review Manual 15th Edition, page 82-831; 2: How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria - Gartner2

Question: 158

Which of the following BEST facilitates an information security manager's efforts to obtain senior management commitment for an information security program?

A. Presenting evidence of inherent risk
B. Reporting the security maturity level
C. Presenting compliance requirements
D. Communicating the residual risk

Answer: D

Explanation:

Communicating the residual risk is the best way to facilitate an information security manager's efforts to obtain senior management commitment for an information security program. The residual risk is the level of risk that remains after applying the security controls and mitigation measures. The residual risk reflects the effectiveness and efficiency of the information security program, as well as the potential impact and exposure of the organization. The information security manager should communicate the residual risk to the senior management in a clear, concise, and relevant manner, using quantitative or qualitative methods, such as risk matrices, heat maps, dashboards, or reports. The communication of the residual risk should also include the comparison with the inherent risk, which is the level of risk before applying any security controls, and the risk appetite, which is the level of risk that the organization is willing to accept. The communication of the residual risk should help the senior management to understand the value and performance of the information security program, as well as the need and justification for further investment or improvement. Presenting evidence of inherent risk, reporting the security maturity level, and presenting compliance requirements are all important aspects of the information security program, but they are not the best ways to obtain senior management commitment. These aspects may not directly demonstrate the benefits or outcomes of the information security program, or they may not align with the business objectives or priorities of the organization. For example, presenting evidence of inherent risk may show the potential threats and vulnerabilities that the organization faces, but it may not indicate how the information security program addresses or reduces them. Reporting the security maturity level may show the progress and status of the information security program, but it may not relate to the risk level or the business impact. Presenting compliance requirements may show the legal or regulatory obligations that the organization must fulfill, but it may not reflect the actual security needs or goals of the organization. Therefore, communicating the residual risk is the best way to obtain senior management commitment for an information security program, as it shows the results and value of the information security program for the organization. Reference = CISM Review Manual 2023, page 41 1; CISM Practice Quiz 2

Question: 159

An organization's disaster recovery plan (DRP) is documented and kept at a disaster recovery site. Which of the following is the BEST way to ensure the plan can be carried out in an emergency?

A. Store disaster recovery documentation in a public cloud.
B. Maintain an outsourced contact center in another country.
C. Require disaster recovery documentation be stored with all key decision makers.
D. Provide annual disaster recovery training to appropriate staff.

Answer: D

Explanation:

= The best way to ensure that the disaster recovery plan (DRP) can be carried out in an emergency is to provide annual disaster recovery training to the appropriate staff, such as the disaster recovery team, the business process owners, and the IT staff. Disaster recovery training is a process of educating and preparing the staff for their roles, responsibilities, and actions in the event of a disaster that affects the availability, integrity, or

confidentiality of the information assets and systems

that support the business processes and functions. Disaster recovery training can help to ensure that the staff are aware, capable, and confident to execute the DRP, as well as to minimize the impact and damage to the business continuity, reputation, and value. Disaster recovery training can also help to evaluate the adequacy, accuracy, and applicability of the DRP, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the disaster recovery process. Disaster recovery training can also help to document and report the training details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the DRP and the training process.

Storing disaster recovery documentation in a public cloud, maintaining an outsourced contact center in another country, and requiring disaster recovery documentation be stored with all key decision makers are all possible ways to ensure the availability and accessibility of the DRP in an emergency, but they are not the best ones. Storing disaster recovery documentation in a public cloud is a process of using a third-party service provider to store and manage the DRP documents online, which can offer benefits such as scalability, flexibility, and cost-efficiency, but also risks such as data breach, data loss, or service disruption. Maintaining an outsourced contact center in another country is a process of using a third-party service provider to handle the communication and coordination of the disaster recovery process with the internal and external stakeholders, such as the customers, partners, or regulators, which can offer benefits such as redundancy, reliability, and expertise, but also risks such as cultural, legal, or contractual issues. Requiring disaster recovery documentation be stored with all key decision makers is a process of ensuring that the senior management and the business process owners have a copy of the DRP documents, which can offer benefits such as accountability, authority, and visibility, but also risks such as inconsistency, duplication, or unauthorized access. Reference = CISM Review Manual 15th Edition, pages 233-2341; CISM Practice Quiz, question 1602

Question: 160

Reevaluation of risk is MOST critical when there is:

A. resistance to the implementation of mitigating controls.
B. a management request for updated security reports.
C. a change in security policy.
D. a change in the threat landscape.

Answer: D

Explanation:

= Reevaluation of risk is a vital aspect of the risk management process that helps organizations to identify and analyze new or evolving threats, vulnerabilities, and impacts on their assets, and implement the necessary controls to mitigate them. Reevaluation of risk is most critical when there is a change in the threat landscape, which refers to the external and internal factors that influence the likelihood and severity of potential attacks on the organization's information assets. A change in the threat landscape may be caused by various factors, such as technological innovations, geopolitical events, cybercrime trends, regulatory changes, or organizational changes. A change in the threat landscape may introduce new risks or alter the existing risk profile of the organization, requiring a reassessment of the risk appetite, tolerance, and strategy. Reevaluation of risk helps the

organization to adapt to the changing threat landscape and ensure that the information security program

remains effective, efficient, and aligned with the business objectives.

Reference =

CISM Review Manual 15th Edition, page 1131

CISM Domain 2: Information Risk Management (IRM) [2022 update]2

Reevaluation of Risk | CISM Exam Question Answer | ISACA3

Question: 161

Which of the following is MOST effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application?

A. A patch management process
B. Version control
C. Change management controls
D. Logical access controls

Answer: A

Explanation:

= Change management controls are the most effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application. Change management controls are the policies, procedures, and practices that govern the initiation, approval, implementation, testing, and documentation of changes to the information systems and infrastructure. Change management controls help to ensure that changes are authorized, planned, controlled, and monitored, and that they do not introduce any unintended or adverse effects on the security, functionality, performance, or reliability of the system or application. Change management controls also help to identify and mitigate any potential risks or issues that may arise from the changes, and to ensure that the changes are aligned with the business objectives and requirements. By implementing change management controls, the organization can prevent the introduction of vulnerabilities that may disrupt the availability of a critical business application, as well as enhance the quality and efficiency of the change process. Reference = CISM Review Manual 15th Edition, page 105, page 106.

Question: 162

An organization is creating a risk mitigation plan that considers redundant power supplies to reduce the business risk associated with critical system outages. Which type of control is being considered?

A. Preventive
B. Corrective
C. Detective
D. Deterrent

Answer: A

Explanation:

A preventive control is a type of control that aims to prevent or reduce the occurrence or impact of potential adverse events that can affect the organization's objectives and performance. Preventive controls are proactive measures that are implemented before an incident happens, and they are designed to address the root causes or sources of risk. Preventive controls can also help the organization to comply with the relevant laws, regulations, standards, and best practices regarding information security1.

An example of a preventive control is a redundant power supply, which is a backup or alternative source of power that can be used in case of a power outage or failure. A redundant power supply can reduce the business risk associated with critical system outages, which can result from power disruptions caused by natural disasters, technical faults, human errors, or malicious attacks. A redundant power supply can provide the following benefits for information security2: Maintain the availability and continuity of the critical systems and services that depend on power, such as servers, databases, networks, or applications. A redundant power supply can ensure that the critical systems and services can operate normally or resume quickly after a power outage or failure, minimizing the downtime and data loss that can affect the organization's operations, customers, or reputation.

Protect the integrity and reliability of the critical systems and data that are stored or processed by the power-dependent devices, such as computers, hard drives, or memory cards. A redundant power supply can prevent or reduce the damage or corruption of the critical systems and data that can be caused by sudden or unexpected power fluctuations, surges, or interruptions, which can compromise the accuracy, completeness, or consistency of the information.

Enhance the resilience and redundancy of the power infrastructure and network that supports the critical systems and services. A redundant power supply can provide an alternative or backup route for power delivery and distribution, which can increase the flexibility and adaptability of the power infrastructure and network to cope with different scenarios or conditions of power supply or demand.

The other options are not the type of control that is being considered by the organization. A corrective control is a type of control that aims to restore or recover the normal state or function of the affected systems or processes after an incident has occurred. A corrective control is a reactive measure that is implemented during or after an incident, and it is designed to address the consequences or impacts of risk. A corrective control can also help the organization to learn from the incident and improve its information security practices1. An example of a corrective control is a backup or restore system, which is a method of creating and restoring copies of the system or data that have been lost or damaged due to an incident.

A detective control is a type of control that aims to identify or discover the occurrence or existence of an incident or a deviation from the expected or desired state or behavior of the systems or processes. A detective control is a monitoring or auditing measure that is implemented during or after an incident, and it is designed to provide information or evidence of risk. A detective control can also help the organization to analyze or investigate the incident and determine the root cause or source of risk1. An example of a detective control is a log or alert system, which is a tool of recording or reporting the activities or events that have occurred or are occurring within the systems or processes.

A deterrent control is a type of control that aims to discourage or dissuade the potential perpetrators or sources of risk from initiating or continuing an incident or an attack. A deterrent control is a psychological or behavioral measure that is implemented before or during an incident, and it is designed to influence or manipulate the motivation or intention of risk. A deterrent control can also help the organization to reduce the likelihood or frequency of incidents or attacks1. An example of a deterrent control is a warning or notification system, which is a method of communicating or displaying the consequences or penalties of violating the information security policies or rules. Reference = Risk Control Techniques: Preventive, Corrective, Directive, And …, Learn Different types of Security Controls in CISSP - Eduonix Blog

Question: 163

What is the PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes?

A. Security incident reporting procedures are followed.
B. Security staff turnover is reduced.
C. Information assets are classified appropriately.
D. Access is granted based on task requirements.

Answer: D

Explanation:

The PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes is that access is granted based on task requirements. This means that the organization can ensure that the employees have the appropriate level and scope of access to the information assets and systems that they need to perform their duties, and that the access is granted, reviewed, and revoked in accordance with the security policies and standards. This can help to reduce the risk of unauthorized access, misuse, or leakage of information, as well as to comply with the principle of least privilege and the segregation of duties12. Security incident reporting procedures are followed (A) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Security incident reporting procedures are the steps and guidelines that the employees should follow when they detect, report, or respond to a security incident.

Aligning the information security program requirements with the employment and staffing processes can help to ensure that the employees are aware of and trained on the security incident reporting procedures, and that they are enforced and monitored by the management. This can help to improve the effectiveness and efficiency of the incident response process, as well as to comply with the legal and contractual obligations12. Security staff turnover is reduced (B) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Security staff turnover is the rate at which the security personnel leave or join the organization. Aligning the information security program requirements with the employment and staffing processes can help to reduce the security staff turnover by ensuring that the security roles and responsibilities are clearly defined and communicated, that the security personnel are adequately compensated and motivated, and that the security personnel are evaluated and developed regularly. This can help to retain the security talent and expertise, as well as to reduce the costs and risks associated with the security staff turnover12. Information assets are classified appropriately © is a benefit to an organization when information security program

requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Information asset classification is the process of assigning a security level or category to the information assets based on their value, sensitivity, and criticality to the organization. Aligning the information security program requirements with the employment and staffing processes can help to ensure that the information assets are classified appropriately by establishing the ownership and custody of the information assets, the criteria and methods for the information asset classification, and the roles and responsibilities for the information asset classification. This can help to protect the information assets according to their security level or category, as well as to comply with the regulatory and contractual requirements12. Reference = 1: CISM Review Manual 15th Edition, page 75-76, 81-82, 88-89, 93-941; 2: CISM Domain 1: Information Security Governance (ISG) [2022 update]2

Question: 164

An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?

A. Document risk acceptances.
B. Revise the organization's security policy.
C. Assess the consequences of noncompliance.
D. Conduct an information security audit.

Answer: C

Explanation:

Assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard. The information security manager should evaluate the potential impact and exposure of the organization due to the noncompliance with the security standard. The assessment should consider the legal, regulatory, contractual, and reputational implications of the noncompliance, as well as the likelihood and severity of the incidents or penalties that may result from the noncompliance. The assessment should also compare the cost and benefit of complying with the security standard versus accepting the risk of noncompliance. The assessment should provide the basis for making informed and rational decisions about how to address the noncompliance issue and prioritize the actions and resources needed to achieve compliance. Documenting risk acceptances, revising the organization's security policy, and conducting an information security audit are all possible actions that may be taken to address the noncompliance issue, but they are not the next steps that should be done. These actions should be performed after assessing the consequences of noncompliance, and based on the results and recommendations of the assessment. Documenting risk acceptances may be appropriate if the organization decides to accept the risk of noncompliance, and if the risk is within the risk appetite and tolerance of the organization. Revising the organization's security policy may be necessary if the organization decides to comply with the security standard, and if the policy needs to be updated to reflect the new requirements and expectations. Conducting an information security audit may be useful if the organization wants to verify the level of compliance and identify the gaps and weaknesses in the security controls and processes. Therefore, assessing the consequences of noncompliance is the next

step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard, as it helps the information security manager to understand the risk and impact of the noncompliance and to make informed and rational decisions about how to address it.
Reference = CISM Review Manual 2023, page 43 1; CISM Practice Quiz 2

Question: 165

To confirm that a third-party provider complies with an organization's information security requirements, it is MOST important to ensure:

A. security metrics are included in the service level agreement (SLA).
B. contract clauses comply with the organization's information security policy.
C. the information security policy of the third-party service provider is reviewed.

D. right to audit is included in the service level agreement (SLA).

Answer: D

Explanation:

= To confirm that a third-party provider complies with an organization's information security requirements, it is most important to ensure that the right to audit is included in the service level agreement (SLA), which is a contract that defines the scope, quality, and terms of the services that the third-party provider delivers to the organization. The right to audit is a clause that grants the organization the authority and opportunity to inspect and verify the third-party provider's security policies, procedures, controls, and performance, either by itself or by an independent auditor, at any time during the contract period or after a security incident. The right to audit can help to ensure that the third-party provider adheres to the organization's information security requirements, as well as to the legal and regulatory standards and obligations, and that the organization can monitor and measure the security risks and issues that arise from the outsourcing relationship. The right to audit can also help to identify and address any gaps, weaknesses, or errors that could compromise the security of the information assets and systems that are shared, stored, or processed by the third- party provider, and to provide feedback and recommendations for improvement and optimization of the security posture and performance.

Security metrics, contract clauses, and the information security policy of the third-party provider are all important elements of ensuring the compliance of the third-party provider with the organization's information security requirements, but they are not the most important ones. Security metrics are quantitative and qualitative measures that indicate the effectiveness and efficiency of the security controls and processes that the third-party provider implements and reports to the organization, such as the number of security incidents, the time to resolve them, the level of customer satisfaction, or the compliance rate. Security metrics can help to evaluate and compare the security performance and outcomes of the third-party provider, as well as to identify and address any deviations or discrepancies from the expected or agreed levels. Contract clauses are legal and contractual terms and conditions that bind the third-party provider to the organization's information security requirements, such as the confidentiality, integrity, and availability of the information assets and systems, the roles and responsibilities of the parties, the liabilities and penalties for breach or violation, or the dispute resolution mechanisms. Contract clauses can help to enforce and protect the organization's information security interests and rights, as well as to prevent or resolve any conflicts or issues that arise from the outsourcing relationship. The information security policy of the third- party provider is a document that defines and communicates the third-party provider's security vision, mission, objectives, and principles, as well as the security roles, responsibilities, and rules that apply to the third-party provider's staff, customers, and partners. The information security policy of the third-party provider can help to ensure that the third-party provider has a clear and consistent security direction and guidance, as well as to align and integrate the third-party provider's security practices and culture with the organization's security expectations and requirements. Reference = CISM Review Manual 15th Edition, pages 57-581; CISM Practice Quiz, question 1662

Question: 166

Which of the following is MOST important to include in monthly information security reports to the board?

A. Trend analysis of security metrics

B. Risk assessment results
C. Root cause analysis of security incidents
D. Threat intelligence

Answer: A

Explanation:

The most important information to include in monthly information security reports to the board is the trend analysis of security metrics. Security metrics are quantitative and qualitative measures that indicate the performance and effectiveness of the information security program and the alignment with the business objectives. Trend analysis is the process of comparing and evaluating the changes and patterns of security metrics over time. Trend analysis can help to identify the strengths and weaknesses of the information security program, the progress and achievements of the security goals and initiatives, the gaps and opportunities for improvement, and the impact and value of the information security investments. Trend analysis can also help to communicate the current and future security risks and challenges, and the recommended actions and strategies to address them. Trend analysis can provide the board with a clear and concise overview of the information security status and direction, and enable informed and timely decision making.
Reference =
CISM Review Manual 15th Edition, page 1631
The CISO's Guide to Reporting Cybersecurity to the Board2
CISM 2020: Information Security Metrics and Reporting, video 13

Question: 167

Which of the following should be the PRIMARY basis for determining the value of assets?

A. Cost of replacing the assets
B. Business cost when assets are not available
C. Original cost of the assets minus depreciation
D. Total cost of ownership (TCO)

Answer: B

Explanation:

The primary basis for determining the value of assets should be the business cost when assets are not available. This is because the value of assets is not only determined by their acquisition or replacement cost, but also by their contribution to the organization's business objectives and processes. The business cost when assets are not available reflects the potential impact of losing or compromising the assets on the organization's operations, performance, reputation, and compliance. The business cost when assets are not available can be estimated by conducting a business impact analysis (BIA), which identifies the criticality, dependencies, and recovery requirements of the assets. By using the business cost when assets are not available as the primary basis for determining the value of assets, the organization can prioritize the protection and management of the assets according to their importance and risk level. Reference = CISM Review Manual 15th Edition, page 64, page 65.

Question: 168

Which of the following BEST enables the integration of information security governance into corporate governance?

A. Well-decumented information security policies and standards
B. An information security steering committee with business representation
C. Clear lines of authority across the organization
D. Senior management approval of the information security strategy

Answer: B

Explanation:

= The best way to enable the integration of information security governance into corporate governance is to establish an information security steering committee with business representation. An information security steering committee is a group of senior executives and managers from different business units and functions who are responsible for overseeing, directing, and supporting the information security program and strategy of the organization. An information security steering committee with business representation can enable the integration of information security governance into corporate governance by providing the following benefits12:

Align the information security objectives and priorities with the business objectives and priorities, and ensure that the information security program and strategy support and enable the achievement of the organizational goals and performance.

Communicate and promote the value and importance of information security to the board of directors, senior management, and other stakeholders, and ensure that information security is considered and incorporated in the decision making and planning processes of the organization.

Provide guidance and direction to the information security manager and the information security team, and ensure that they have the necessary authority, resources, and support to implement and maintain the information security program and strategy effectively and efficiently.

Monitor and evaluate the performance and outcomes of the information security program and strategy, and ensure that they are aligned with the expectations and requirements of the organization and its stakeholders, as well as the relevant laws, regulations, standards, and best practices.

Identify and address the issues, challenges, and opportunities related to information security, and ensure that the information security program and strategy are continuously improved and updated to reflect the changes and developments in the internal and external environment.

The other options are not the best way to enable the integration of information security governance into corporate governance, as they are less comprehensive, effective, or influential than establishing an information security steering committee with business representation. Well-documented information security policies and standards are important components of the information security program and strategy, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not reflect or align with the business needs, priorities, or expectations, and they may not be communicated, implemented, or enforced properly or consistently across the organization. Clear lines of authority across the organization are important factors for the information security governance structure, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not ensure the involvement, participation, or support of the senior executives, managers, and other

stakeholders who are responsible for or affected by information security. Senior management approval of the information security strategy is an important outcome of the information security governance process, but it is not sufficient to enable the integration of information security governance into corporate governance, as it may not ensure the alignment, communication, or monitoring of the information security strategy with the business strategy, and it may not ensure the accountability, responsibility, or authority of the information security manager and the information security team12. Reference = CISM Domain 1: Information Security Governance (ISG) [2022 update], Information Security Governance for CISM® | Pluralsight, Aligning Information Security with Business Strategy - ISACA, Aligning Information Security with Business Objectives - ISACA

Question: 169

Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?

A. Existence of a right-to-audit clause
B. Results of the provider's business continuity tests
C. Technical capabilities of the provider
D. Existence of the provider's incident response plan

Answer: C

Explanation:

The technical capabilities of the provider are the MOST important thing for an information security manager to verify when selecting a third-party forensics provider because they determine the

quality, reliability, and validity of the forensic services and results that the provider can deliver. The technical capabilities of the provider include the skills, experience, and qualifications of the forensic staff, the methods, tools, and standards that the forensic staff use, and the facilities, equipment, and resources that the forensic staff have. The information security manager should verify that the technical capabilities of the provider match the forensic needs and expectations of the organization, such as the type, scope, and complexity of the forensic investigation, the legal and regulatory requirements, and the time and cost constraints12. The existence of a right-to-audit clause (A) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. A right-to-audit clause is a contractual provision that grants the organization the right to audit or review the performance, compliance, and security of the provider. A right-to-audit clause can help to ensure the accountability, transparency, and quality of the provider, as well as to identify and resolve any issues or disputes that may arise during or after the forensic service. However, a right-to-audit clause does not guarantee that the provider has the technical capabilities to conduct the forensic service effectively and efficiently12. The results of the provider's business continuity tests (B) are an important thing for an information security manager to verify when selecting a third-party forensics provider, but they are not the MOST important thing. The results of the provider's business continuity tests can indicate the ability and readiness of the provider to continue or resume the forensic service in the event of a disruption, disaster, or emergency. The results of the provider's business continuity tests can help to assess the availability, resilience, and recovery of the provider, as well as to mitigate the risks of losing or compromising the forensic evidence or data. However, the results of the provider's business continuity tests do not ensure that the provider has the technical capabilities to perform the forensic service accurately and professionally12. The existence of the provider's incident response plan (D) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. The

existence of the provider's incident response plan can demonstrate the preparedness and capability of the provider to detect, report, and respond to any security incidents that may affect the forensic service or the organization. The existence of the provider's incident response plan can help to protect the confidentiality, integrity, and availability of the forensic evidence or data, as well as to comply with the legal and contractual obligations. However, the existence of the provider's incident response plan does not confirm that the provider has the technical capabilities to execute the forensic service competently and ethically12. Reference = 1: CISM Review Manual 15th Edition, page 310-3111; 2: A Risk-Based Management Approach to Third- Party Data Security, Risk and Compliance - ISACA2

Question: 170

Of the following, whose input is of GREATEST importance in the development of an information security strategy?

A. Process owners
B. End users
C. Security architects.
D. Corporate auditors

Answer: A

Explanation:

Process owners are the people who are responsible for the design, execution, and improvement of the business processes that support the organization's objectives and operations. Process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Process owners also help to identify and assess the risks and impacts that the business processes face, and to define and implement the security controls and measures that can mitigate or reduce them. Process owners also facilitate the alignment and integration of the information security strategy with the business strategy, as well as the communication and collaboration among the various stakeholders and functions involved in the information security program. End users, security architects, and corporate auditors are all important stakeholders in the information security program, but they do not have the greatest importance in the development of an information security strategy. End users are the people who use the information systems and services that the information security program protects and enables. End users provide the input and feedback on the usability, functionality, and performance of the information systems and services, as well as the security awareness and behavior that they exhibit. Security architects are the people who design and implement the security architecture that supports the information security strategy. Security architects provide the input and feedback on the technical requirements, capabilities, and solutions that the information security strategy should leverage and optimize. Corporate auditors are the people who evaluate and verify the compliance and effectiveness of the information security program. Corporate auditors provide the input and feedback on the standards, regulations, and best practices that the information security strategy should follow and adhere to. Therefore, process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Reference = CISM Review Manual 2023, page 31 1; CISM Practice Quiz 2

Question: 171

When performing a business impact analysis (BIA), who should calculate the recovery time and cost estimates?

A. Business process owner
B. Business continuity coordinator
C. Senior management
D. Information security manager

Answer: A

Explanation:

The business process owner is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The business process owner has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the business process owner is the best person to calculate the recovery time and cost estimates when performing a business impact analysis (BIA), which is a process of identifying and

quantifying the potential losses, damages, or consequences that could result from a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The recovery time and cost estimates are the measures that indicate the time and money that are needed to resume and restore the normal business operations and functions after the disruption or incident. The recovery time and cost estimates can help to prioritize and protect the critical activities and resources, to allocate the appropriate budget and resources, to implement the necessary controls and measures, and to evaluate the effectiveness and efficiency of the business continuity and disaster recovery plans.

The business continuity coordinator, the senior management, and the information security manager are all important roles in the BIA process, but they are not the best ones to calculate the recovery time and cost estimates. The business continuity coordinator is the person who is responsible for coordinating and facilitating the BIA process, as well as the development, implementation, and maintenance of the business continuity and disaster recovery plans. The business continuity coordinator can help to define and communicate the scope, objectives, and methodology of the BIA, to collect and analyze the data and information from the business process owners and other stakeholders, to report and present the BIA results and recommendations, and to provide feedback and suggestions for improvement and optimization of the BIA and the plans. The senior management is the group of people who have the ultimate authority and accountability for the organization's strategy, direction, and performance. The senior management can help to approve and support the BIA process and the plans, to provide the strategic guidance and vision for the business continuity and disaster recovery, to allocate the necessary budget and resources, to oversee and monitor the BIA and the plans, and to make the final decisions and approvals. The information security manager is the person who is responsible for ensuring the security of the information assets and systems that support the business processes and functions. The information security manager can help to identify and assess the information security risks and issues that could affect the BIA and the plans, to implement and manage the security controls and measures that are needed to protect and recover the information assets and systems, to coordinate and collaborate with the business process owners and other stakeholders on the security aspects of the BIA and the plans, and to provide the security expertise and advice. Reference = CISM Review Manual 15th Edition, pages 2282291;

Question: 172

Which of the following BEST indicates the effectiveness of a recent information security awareness campaign delivered across the organization?

A. Decrease in the number of security incidents
B. Increase in the frequency of security incident escalations
C. Reduction in the impact of security incidents
D. Increase in the number of reported security incidents

Answer: D

Explanation:

The best indicator of the effectiveness of a recent information security awareness campaign delivered across the organization is the increase in the number of reported security incidents. This

means that the employees have become more aware of the security threats and issues, and have learned how to recognize and report them to the appropriate authorities. Reporting security incidents is a vital part of the incident response process, as it helps to identify and contain the incidents, prevent further damage, and initiate the recovery actions. Reporting security incidents also helps to collect and analyze the incident data, which can be used to improve the security controls and policies, and to prevent or mitigate similar incidents in the future. An increase in the number of reported security incidents shows that the awareness campaign has successfully raised the level of security knowledge, attitude, and behavior among the employees, and has encouraged them to take an active role in protecting the organization's information assets.

Reference =

CISM Review Manual 15th Edition, page 1631

Measuring and Evaluating the Effectiveness of Security Awareness Improvement Methods2 Developing metrics to assess the effectiveness of cybersecurity awareness program3 How to build a successful information security awareness programme - BCS4

How to Increase Cybersecurity Awareness - ISACA5

Question: 173

Which of the following should be the MOST important consideration of business continuity management?

A. Ensuring human safety
B. Identifying critical business processes
C. Ensuring the reliability of backup data
D. Securing critical information assets

Answer: A

Explanation:

= Business continuity management (BCM) is the process of planning and implementing measures to ensure the continuity of critical business processes in the event of a disruption. The most important consideration of BCM is ensuring human safety, as this is the primary responsibility of any organization and the basis of ethical conduct. Human safety includes protecting the health and wellbeing of employees, customers, suppliers, and other stakeholders who may be affected by a disruption. Identifying critical business processes, ensuring the reliability of backup data, and securing critical information assets are also important aspects of BCM, but they are secondary to human safety. Reference = CISM Review Manual, 16th Edition, ISACA, 2020, p. 2111; CISM Online Review Course, Domain 4: Information Security Incident Management, Module 4: Business Continuity and Disaster Recovery, ISACA2

Question: 174

A user reports a stolen personal mobile device that stores sensitive corporate dat a. Which of the following will BEST minimize the risk of data exposure?

A. Prevent the user from using personal mobile devices.

B. Report the incident to the police.

C. Wipe the device remotely.

D. Remove user's access to corporate data.

Answer: C

Explanation:

Wiping the device remotely is the best option to minimize the risk of data exposure from a stolen personal mobile device. This action will erase all the data stored on the device, including the sensitive corporate data, and prevent unauthorized access or misuse. Wiping the device remotely can be done using enterprise mobility management (EMM) or mobile device management (MDM) tools that allow administrators to remotely manage and secure mobile devices. Alternatively, some mobile devices have built-in features that allow users to wipe their own devices remotely using another device or a web portal.

Preventing the user from using personal mobile devices is not a feasible option, as it may affect the user's productivity and convenience. Moreover, this option does not address the immediate risk of data exposure from the stolen device.

Reporting the incident to the police is a good practice, but it does not guarantee that the device will be recovered or that the data will be protected. The police may not have the resources or the authority to track down the device or access it.

Removing the user's access to corporate data is a preventive measure that can limit the damage caused by a stolen device, but it does not eliminate the risk of data exposure from the data already stored on the device. The user may have cached or downloaded data that can still be accessed by an attacker even if the user's access is revoked. Reference =

Guidelines for Managing the Security of Mobile Devices in the Enterprise NIST Special Publication, Section 3.1.11, page 3-8

CISM Review Manual, Chapter 3, page 121

Mobile device security - CISM Certification Domain 2: Information Risk Management Video Boot Camp 2019, Section 3.3, 00:03:10

Question: 175

Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?

A. Regulatory requirements are being met.
B. Internal compliance requirements are being met.
C. Risk management objectives are being met.
D. Business needs are being met.

Answer: D

Explanation:

The primary purpose of business continuity and disaster recovery plans is to ensure that the organization can resume its critical business functions within the stated recovery time objectives (RTOs) after a disruptive event. RTOs are based on the business needs and the impact analysis of each function or process. Therefore, meeting the business needs is the best indicator that the plans are effective. Regulatory requirements, internal compliance requirements, and risk management objectives are important factors that influence the development and testing of the plans, but they are not the ultimate measure of their effectiveness. Reference = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3071; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Imperva, Business Continuity & Disaster Recovery Planning (BCP & DRP)3

Question: 176

Which of the following is the BEST approach to incident response for an organization migrating to a cloud-based solution?

A. Adopt the cloud provider's incident response procedures.
B. Transfer responsibility for incident response to the cloud provider.
C. Continue using the existing incident response procedures.
D. Revise incident response procedures to encompass the cloud environment.

Answer: D

Explanation:

The best approach to incident response for an organization migrating to a cloud-based solution is to revise the existing incident response procedures to encompass the cloud environment. This is because the cloud environment introduces new challenges and risks that may not be adequately addressed by the current procedures. For example, the cloud provider may have different roles and responsibilities, service level agreements, notification and escalation processes, data protection and privacy requirements, and legal and regulatory obligations than the organization. Therefore, the organization should review and update its incident

response procedures to align with the cloud provider's policies and practices, as well as the organization's business objectives and risk appetite. The organization should also ensure that the incident response team members are trained and aware of the changes in the procedures and the cloud environment.

The other options are not the best approaches because they do not consider the specific characteristics and implications of the cloud environment. Adopting the cloud provider's incident response procedures may not be feasible or desirable, as the organization may have different needs and expectations than the cloud provider. Transferring responsibility for incident response to the cloud provider may not be possible or advisable, as the organization may still retain some accountability and liability for the security and availability of its data and services in the cloud. Continuing to use the existing incident response procedures may not be effective or efficient, as the procedures may not cover the scenarios and issues that may arise in the cloud environment. Reference =

CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-192, 195-196, 199-200.

Cloud Incident Response Framework – A Quick Guide 2, pages 3-4, 6-7, 9-10.

CISM ITEM DEVELOPMENT GUIDE 3, page 18, Question 1.

Question: 177

Which of the following is the BEST indication of effective information security governance?

A. Information security is considered the responsibility of the entire information security team.
B. Information security controls are assigned to risk owners.
C. Information security is integrated into corporate governance.
D. Information security governance is based on an external security framework.

Answer: C

Explanation:

Information security governance (ISG) is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk1. Effective ISG ensures that information security is integrated into corporate governance and is considered an essential component of enterprise governance2. Information security is not just the responsibility of the information security team, but of all stakeholders in the organization3. Information security controls are not assigned to risk owners, but to control owners who are accountable for implementing and maintaining the controls4. Information security governance is not based on an external security framework, but on the organization's own objectives, risk appetite, and compliance requirements. Reference = 1: CISM Review Manual (Digital Version), page 3 2: CISM Review Manual (Digital Version), page 4 3: CISM Review Manual (Digital Version), page 5 4: CISM Review Manual (Digital Version), page 14 : CISM Review Manual (Digital Version), page 16

Question: 178

Which of the following is the BEST way to assess the risk associated with using a Software as a Service (SaaS) vendor?

A. Verify that information security requirements are included in the contract.
B. Request customer references from the vendor.
C. Require vendors to complete information security questionnaires.
D. Review the results of the vendor's independent control reports.

Answer: D

Explanation:

Reviewing the results of the vendor's independent control reports is the best way to assess the risk associated with using a SaaS vendor because it provides an objective and reliable evaluation of the

vendor's security controls and practices. Independent control reports, such as SOC 2 or ISO 27001, are conducted by third-party auditors who verify the vendor's compliance with industry standards and best practices. These reports can help the customer identify any gaps or weaknesses in the vendor's security posture and determine the level of assurance and trust they can place on the vendor.

Verifying that information security requirements are included in the contract is a good practice, but it does not provide sufficient assurance that the vendor is actually meeting those requirements. The contract may also have limitations or exclusions that reduce the customer's rights or remedies in case of a breach or incident.

Requesting customer references from the vendor is not a reliable way to assess the risk associated with using a SaaS vendor because the vendor may only provide positive or biased references that do not reflect the true experience or satisfaction of the customers. Customer references may also not have the same security needs or expectations as the customer who is conducting the assessment. Requiring vendors to complete information security questionnaires is a useful way to gather information about the vendor's security policies and procedures, but it does not provide enough evidence or verification that the vendor is actually implementing and maintaining those policies and procedures. Information security questionnaires are also subject to the vendor's self-reporting and interpretation, which may not be accurate or consistent. Reference = CISM Review Manual 15th Edition, page 144

SaaS Security Risk and Challenges - ISACA1

SaaS Security Checklist & Assessment Questionnaire | LeanIX2

Risk Assessment Guide for Microsoft Cloud3

Question: 179

Which of the following is a PRIMARY benefit of managed security solutions?

A. Wider range of capabilities
B. Easier implementation across an organization
C. Greater ability to focus on core business operations
D. Lower cost of operations

Answer: C

Explanation:

Managed security solutions are services provided by external vendors that offer security expertise, resources, and tools to help organizations protect their information assets and systems. A primary benefit of managed security solutions is that they allow organizations to focus on their core business operations, while delegating the security tasks to the service provider. This can improve the efficiency and effectiveness of the organization, as well as reduce the complexity and cost of managing security internally. Managed security solutions can also provide a wider range of capabilities, easier implementation across an organization, and lower cost of operations, but these are not the primary benefits, as they may vary depending on the quality and scope of the service provider. Reference = CISM Review Manual, 16th Edition, ISACA, 2020, p. 841; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 3: Information Security Program Management, ISACA2

Question: 180

Which of the following is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model?

A. Host patching
B. Penetration testing
C. Infrastructure hardening
D. Data classification

Answer: D

Explanation:

Data classification is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model. Data classification is the process of categorizing data based on its sensitivity, value and criticality to the organization. Data classification helps to determine the appropriate level of protection, access control and retention for different types of data. Data classification is an essential part of data governance and risk management, as it enables the organization to comply with legal and regulatory requirements, protect its intellectual property and reputation, and optimize its data storage and usage costs.

In a SaaS model, the client organization has the least control and responsibility over the cloud infrastructure, platform and application, as these are fully managed by the cloud service provider (CSP). The client organization only has control and responsibility over its own data and users. Therefore, the client organization is responsible for defining and implementing data classification policies and procedures, and ensuring that its data is properly labeled and handled according to its classification level. The client organization is also responsible for educating its users about the importance of data classification and the best practices for data security and privacy.

The other options are not the sole responsibility of the client organization in a SaaS model, as they are either shared with or delegated to the CSP. Host patching, penetration testing and infrastructure hardening are all related to the security and maintenance of the cloud infrastructure and platform, which are the responsibility of the CSP in a SaaS model. The CSP is expected to provide regular updates, patches and fixes to the host operating system, network and application components, and to conduct periodic security assessments and audits to identify and remediate any vulnerabilities or weaknesses in the cloud environment. The client organization may have some responsibility to monitor and verify the CSP's performance and compliance with the service level agreement (SLA) and the cloud security standards and regulations, but it does not have direct control or access to the cloud infrastructure and platform.

Reference =

Understanding the Shared Responsibilities Model in Cloud Services - ISACA, Figure 1 CISM Review Manual, Chapter 3, page 121

Question: 181

Which of the following presents the GREATEST challenge to a security operations center's wna GY of potential security breaches?

A. IT system clocks are not synchronized with the centralized logging server.
B. Operating systems are no longer supported by the vendor.
C. The patch management system does not deploy patches in a timely manner.
D. An organization has a decentralized data center that uses cloud services.

Answer: A

Explanation:

A security operations center (SOC) relies on the centralized logging server to collect, store, analyze and correlate security events from various sources such as firewalls, intrusion detection systems, antivirus software, etc. The centralized logging server uses the timestamps of the events to perform the analysis and correlation. If the IT system clocks are not synchronized with the centralized logging server, the SOC will face difficulties in identifying the sequence and causality of the events, which will affect its ability to detect and respond to potential security breaches. Therefore, this presents the greatest challenge to the SOC's awareness of potential security breaches.

Operating systems that are no longer supported by the vendor may pose a security risk, but they can be mitigated by applying compensating controls such as isolation, segmentation, monitoring, etc. The patch management system that does not deploy patches in a timely manner may also increase the vulnerability exposure, but it can be remediated by prioritizing and applying the critical patches as soon as possible. An organization that has a decentralized data center that uses cloud services may face some challenges in ensuring the security and compliance of the cloud environment, but it can leverage the cloud service provider's security capabilities and tools to enhance the SOC's visibility and control. Therefore, these options are not the greatest challenges to the SOC's awareness of potential security breaches. Reference = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; RSI Security, Common Challenges of SOC Teams3; Infosec Matter, Security Operations Center: Challenges of SOC Teams4

Question: 182

Which of the following defines the triggers within a business continuity plan (BCP)? @

A. Needs of the organization
B. Disaster recovery plan (DRP)
C. Information security policy
D. Gap analysis

Answer: B

Explanation:

The needs of the organization define the triggers within a business continuity plan (BCP). Triggers are the events or conditions that initiate the activation of the BCP. The triggers should be based on

the organization's business objectives, risk appetite, recovery time objectives, and recovery point objectives. The triggers should also be aligned with the organization's information security policy, disaster recovery plan, and gap analysis. However, these are not the primary factors that define the triggers, but rather the supporting elements that help implement the BCP. The needs of the organization are the main drivers for determining the triggers, as they reflect the organization's priorities, expectations, and requirements for business continuity.
Reference =

CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-192, 195-196, 199-200.
Business Continuity Management Guideline 2, page 5, Section 4.2.1: Triggers
Business Continuity Plan - Open Risk Manual 3, page 1, Section 1: Introduction

Question: 183

Following a successful attack, an information security manager should be confident the malware @ continued to spread at the completion of which incident response phase?

A. Containment
B. Recovery
C. Eradication
D. Identification

Answer: A

Explanation:

According to the CISM Review Manual (Digital Version), page 212, the incident response process consists of six phases: preparation, identification, containment, eradication, recovery, and lessons learned. Containment is the phase where the incident response team isolates the affected systems or networks to prevent further damage or spread of the malware. Eradication is the phase where the incident response team removes the malware and any traces of its activity from the affected systems or networks. Recovery is the phase where the incident response team restores the normal operations of the systems or networks. Identification is the phase where the incident response team detects and analyzes the signs of the incident. Therefore, the information security manager should be confident that the malware has not continued to spread at the completion of the containment phase, which is the earliest phase where the incident response team can stop the propagation of the malware. Reference = 1: CISM Review Manual (Digital Version), page 212

Question: 184

Due to specific application requirements, a project team has been granted administrative ponieon GR: is the PRIMARY reason for ensuring clearly defined roles and responsibilities are communicated to these users?

A. Clearer segregation of duties
B. Increased user productivity
C. Increased accountability
D. Fewer security incidents

Answer: C

Explanation:

Increasing accountability is the primary reason for ensuring clearly defined roles and responsibilities are communicated to users who have been granted administrative privileges due to specific application requirements. Administrative privileges grant users the ability to perform actions that can affect the security, availability and integrity of the application or system, such as installing software, modifying configurations, accessing sensitive data or granting access to other users. Therefore, users who have administrative privileges must be aware of their roles and responsibilities and the consequences of their actions. Communicating clearly defined roles and responsibilities to these users helps to establish accountability by setting expectations, defining boundaries, assigning ownership and enabling monitoring and reporting. Accountability also helps to deter misuse or abuse of privileges, ensure compliance with policies and standards, and facilitate incident response and investigation.

Clearer segregation of duties is a benefit of ensuring clearly defined roles and responsibilities, but it is not the primary reason. Segregation of duties is a control that aims to prevent or detect conflicts of interest, errors, fraud or unauthorized activities by separating different functions or tasks among different users or groups. For example, a user who can create a purchase order should not be able to approve it. Segregation of duties helps to reduce the risk of unauthorized or inappropriate actions by requiring more than one person to complete a critical or sensitive process. However, segregation of duties alone does not ensure accountability, as users may still act in collusion or circumvent the control.

Increased user productivity is a possible outcome of ensuring clearly defined roles and responsibilities, but it is not the primary reason. User productivity refers to the efficiency and effectiveness of users in performing their tasks and achieving their goals. By communicating clearly defined roles and responsibilities, users may have a better understanding of their tasks, expectations and performance indicators, which may help them to work faster, smarter and better. However, user productivity is not directly related to the security risk of granting administrative privileges, and it may also depend on other factors, such as user skills, motivation, tools and resources.

Fewer security incidents is a desired result of ensuring clearly defined roles and responsibilities, but it is not the primary reason. Security incidents are events or situations that compromise the confidentiality, integrity or availability of information assets or systems. By communicating clearly defined roles and responsibilities, users may be more aware of the security implications of their actions and the potential threats and vulnerabilities they may face, which may help them to avoid or prevent security incidents. However, fewer security incidents is not a guarantee or a measure of accountability, as users may still cause or experience security incidents due to human error, negligence, malicious intent or external factors. Reference = CISM Review Manual 15th Edition, page 144 Effective User Access Reviews - ISACA1

CISM ITEM DEVELOPMENT GUIDE - ISACA2

Question: 185

An information security manager believes that information has been classified inappropriately, = the

risk of a breach. Which of the following is the information security manager's BEST action?

A. Refer the issue to internal audit for a recommendation.
B. Re-classify the data and increase the security level to meet business risk.
C. Instruct the relevant system owners to reclassify the data.
D. Complete a risk assessment and refer the results to the data owners.

Answer: D

Explanation:

= Information classification is the process of assigning appropriate labels to information assets based on their sensitivity and value to the organization. Information classification should be aligned with the business objectives and risk appetite of the organization, and should be reviewed periodically to ensure its accuracy and relevance. The information security manager is responsible for establishing and maintaining the information classification policy and procedures, as well as providing guidance and oversight to the data owners and custodians. Data owners are the individuals who have the authority and accountability for the information assets within their business unit or function. Data owners are responsible for determining the appropriate classification level and security controls for their information assets, as well as ensuring compliance with the information classification policy and procedures. Data custodians are the individuals who have the operational responsibility for implementing and maintaining the security controls for the information assets assigned to them by the data owners.

If the information security manager believes that information has been classified inappropriately, increasing the risk of a breach, the best action is to complete a risk assessment and refer the results to the data owners. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks associated with the information assets, and recommending appropriate risk treatment options. By conducting a risk assessment, the information security manager can provide objective and evidence-based information to the data owners, highlighting the potential impact and likelihood of a breach, as well as the cost and benefit of implementing additional security controls. This will enable the data owners to make informed decisions about the appropriate classification level and security controls for their information assets, and to justify and document any deviations from the information classification policy and procedures.

The other options are not the best actions for the information security manager. Refering the issue to internal audit for a recommendation is not the best action, because internal audit is an independent and objective assurance function that provides assurance on the effectiveness of governance, risk management, and control processes. Internal audit is not responsible for providing recommendations on information classification, which is a management responsibility. Re-classifying the data and increasing the security level to meet business risk is not the best action, because the information security manager does not have the authority or accountability for the information assets, and may not have the full understanding of the business context and objectives of the data owners. Instructing the relevant system owners to reclassify the data is not the best action, because system owners are not the same as data owners, and may not have the authority or accountability for the information assets either. System owners are the individuals who have the authority and accountability for the information systems that process, store, or transmit the information assets. System owners are responsible for ensuring that the information systems comply with the security requirements and controls defined by the data owners and the information security

manager. Reference = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 49-51, 63-64, 69-701;
CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 2: Information Security Program Framework, ISACA2

Question: 186

Which of the following is the BEST indication of information security strategy alignment with the "&

A. Percentage of information security incidents resolved within defined service level agreements (SLAs)
B. Percentage of corporate budget allocated to information security initiatives
C. Number of business executives who have attended information security awareness sessions
D. Number of business objectives directly supported by information security initiatives

Answer: D

Explanation:

The number of business objectives directly supported by information security initiatives is the best indication of information security strategy alignment with the organizational goals and objectives. This metric shows how well the information security strategy is aligned with the business strategy, and how effectively the information security program is delivering value to the organization. The more business objectives that are supported by information security initiatives, the more aligned the information security strategy is with the organizational goals and objectives.

The other options are not the best indicators of information security strategy alignment, as they do not directly measure the impact or contribution of information security initiatives to the business objectives. The percentage of information security incidents resolved within defined SLAs is a measure of the efficiency and effectiveness of the incident management process, but it does not reflect how well the information security strategy is aligned with the business strategy. The percentage of corporate budget allocated to information security initiatives is a measure of the investment and commitment of the organization to information security, but it does not indicate how well the information security initiatives are aligned with the business objectives or how they are prioritized. The number of business executives who have attended information security awareness sessions is a measure of the awareness and involvement of the senior management in information security, but it does not show how well the information security strategy is aligned with the business strategy or how it supports the business objectives. Reference =

CISM Exam Content Outline | CISM Certification | ISACA, Domain 1, Task 1.1

CISM MASTER CHEAT SHEET - SkillCertPro, Chapter 1, page 2

Certified Information Security Manager (CISM), page 1

Certified Information Security Manager Exam Prep Guide: Aligned with …, page 1

CISM: Certified Information Security SKILLS COVERED Manager, page 1

Question: 187

Which of the following is the BEST way to ensure the capability to restore clean data after a ransomware attack?

A. Purchase cyber insurance
B. Encrypt sensitive production data
C. Perform Integrity checks on backups
D. Maintain multiple ofline backups

Answer: D

Explanation:

The best way to ensure the capability to restore clean data after a ransomware attack is to maintain multiple ofline backups. Ofline backups are backups that are not connected to the network or the internet, and therefore are not accessible by ransomware. Multiple ofline backups provide redundancy and allow the organization to choose the most recent and uncorrupted backup to restore the data. Ofline backups should be stored in a secure location and tested regularly to ensure their integrity and availability.

Purchasing cyber insurance may help the organization cover some of the costs associated with a ransomware attack, such as ransom payment, data recovery, legal fees, etc., but it does not guarantee the capability to restore clean data. Cyber insurance policies may have exclusions, limitations, or conditions that affect the coverage and reimbursement. Moreover, cyber insurance does not prevent or mitigate the ransomware attack itself, and it may not cover all the losses or damages caused by the attack.

Encrypting sensitive production data may protect the confidentiality of the data from unauthorized access or disclosure, but it does not prevent ransomware from encrypting the data again.

Ransomware does not need to decrypt the data to encrypt it, and it may use a different encryption algorithm or key than the one used by the organization. Encrypting production data may also increase the complexity and time required for data recovery, especially if the encryption keys are lost or compromised.

Performing integrity checks on backups may help the organization verify that the backups are not corrupted or tampered with, but it does not ensure the capability to restore clean data after a ransomware attack. Integrity checks are a preventive measure that should be done before the attack, not after. If the backups are already infected or encrypted by ransomware, performing integrity checks will not help to recover the data. Integrity checks should be complemented by other measures, such as isolation, versioning, and ofline storage, to protect the backups from ransomware. Reference = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3081; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Ransomware recovery: 8 steps to successfully restore from backup3; Ransomware Recovery: 5 Steps to Recover Data4

Question: 188

Implementing the principle of least privilege PRIMARILY requires the identification of:

A. job duties
B. data owners
C. primary risk factors.
D. authentication controls

Answer: A

Explanation:

Implementing the principle of least privilege primarily requires the identification of job duties. Job duties are the specific tasks and responsibilities that an individual performs as part of their role in the organization. By

identifying the job duties, the organization can determine the minimum access privileges necessary for each individual to perform their assigned function, and nothing more. This helps to reduce the risk of unauthorized access, misuse, or compromise of information and resources. The principle of least privilege is a key security principle that states that every module (such as a user, a process, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose12.

The other options are not the primary factors that require identification for implementing the principle of least privilege. Data owners are the individuals or entities that have the authority and responsibility to define the classification, usage, and protection of data. Data owners may be involved in granting or revoking access privileges to data, but they are not the ones who identify the job duties of the data users. Primary risk factors are the sources or causes of potential harm or loss to the organization. Primary risk factors may influence the level of access privileges granted to users, but they are not the ones who define the job duties of the users. Authentication controls are the mechanisms that verify the identity of users or systems before granting access to resources. Authentication controls may enforce the principle of least privilege, but they are not the ones who determine the job duties of the users. Reference = Principle of least privilege

What Is the Principle of Least Privilege and Why is it Important? - F5 1 4

Question: 189

Which of the following BEST enables an organization to transform its culture to support information security?

A. Periodic compliance audits
B. Strong management support
C. Robust technical security controls
D. Incentives for security incident reporting

Answer: B

Explanation:

According to the CISM Review Manual (Digital Version), page 5, information security culture is the set of values, attitudes, and behaviors that shape how an organization and its employees view and practice information security. Transforming the information security culture requires a change management process that involves the following steps: creating a sense of urgency, forming a powerful coalition, developing a vision and strategy, communicating the vision, empowering broadbased action, generating short-term wins, consolidating gains and producing more change, and anchoring new approaches in the culture1. Among the four options, strong management support is the best enabler for transforming the information security culture, as it can provide the necessary leadership, resources, sponsorship, and alignment for the change management process. Periodic compliance audits, robust technical security controls, and incentives for security incident reporting are important elements of information security, but they are not sufficient to change the culture without strong management support. Reference = 1: CISM Review Manual (Digital Version), page 5

Question: 190

Which of the following has The GREATEST positive impact on The ability to execute a disaster recovery plan (DRP)?

A. Storing the plan at an offsite location
B. Communicating the plan to all stakeholders
C. Updating the plan periodically
D. Conducting a walk-through of the plan

Answer: D

Explanation:

A walk-through of the disaster recovery plan (DRP) is a method of testing the plan by simulating a disaster scenario and having the participants review their roles and responsibilities, as well as the procedures and resources required to execute the plan. A walk-through has the greatest positive impact on the ability to execute the DRP, as it helps to identify and resolve any gaps, errors, or inconsistencies in the plan, as well as to enhance the awareness and readiness of the stakeholders involved in the recovery process. Reference = CISM Review Manual, 16th Edition, Chapter 5, Section 5.3.2.21

Question: 191

Recovery time objectives (RTOs) are BEST determined by:

A. business managers
B. business continuity officers
C. executive management
D. database administrators (DBAs).

Answer: A

Explanation:

Business managers are best suited to determine the recovery time objectives (RTOs) for their business processes and functions, as they have the knowledge and authority to assess the impact of downtime and the acceptable level of service continuity. RTOs are the maximum acceptable time that a business process or function can be disrupted before it causes significant harm to the organization's objectives, reputation, or compliance. Reference = CISM Review Manual, 16th Edition, Chapter 5, Section 5.2.1.11

Question: 192

Which of the following is MOST effective for communicating forward-looking trends within security reporting?

A. Key control indicator (KCIs)
B. Key risk indicators (KRIs)
C. Key performance indicators (KPIs)
D. Key goal indicators (KGIs)

Answer: B

Explanation:

= Security reporting is the process of providing relevant and timely information on the status and performance of the information security program to the stakeholders. Security reporting should be aligned with the business objectives and risk appetite of the organization, and should provide meaningful insights and recommendations for decision making and improvement. Security reporting should also include forward-looking trends, which are projections or predictions of future events or conditions based on historical data, current situation, and external factors. Forward-looking trends can help the organization anticipate and prepare for potential risks and opportunities, and adjust their strategies and plans accordingly.

One of the most effective ways to communicate forward-looking trends within security reporting is to use key risk indicators (KRIs). KRIs are metrics that measure the level of exposure or likelihood of a risk event occurring, and provide early warning signals of potential changes in the risk profile. KRIs can help the organization monitor and manage the key risks that may affect the achievement of their objectives, and take proactive actions to mitigate or avoid them. KRIs can also help the organization identify emerging risks and trends, and evaluate the effectiveness of their risk treatment options. KRIs should be aligned with the risk appetite and tolerance of the organization, and should be regularly reviewed and updated to reflect the changing risk environment.

The other options are not the most effective ways to communicate forward-looking trends within security reporting. Key control indicators (KCIs) are metrics that measure the effectiveness and efficiency of the security controls implemented to reduce the impact or likelihood of a risk event. KCIs can help the organization assess and improve the performance of their security processes and

activities, and ensure compliance with the security policies and standards. However, KCIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key performance indicators (KPIs) are metrics that measure the achievement of the security objectives and goals, and demonstrate the value and contribution of the information security program to the organization. KPIs can help the organization evaluate and communicate the results and outcomes of their security initiatives and projects, and align them with the business strategy and vision. However, KPIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key goal indicators (KGIs) are metrics that measure the progress and completion of the security goals and targets, and indicate the degree of success and satisfaction of the information security program. KGIs can help the organization track and report the status and milestones of their security plans and actions, and ensure alignment with the stakeholder expectations and requirements. However, KGIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Reference = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 77-78, 81-821; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 4: Information Security Program Resources, ISACA2

Question: 193

The PRIMARY objective of performing a post-incident review is to:

A. re-evaluate the impact of incidents.
B. identify vulnerabilities.
C. identify control improvements.
D. identify the root cause.

Answer: D

Explanation:

= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident. Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of the incident response process, identify lessons learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.

Re-evaluating the impact of incidents is not the primary objective of performing a post-incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re-evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.

Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity, or

availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal.

Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal. Reference =

ISACA CISM: PRIMARY goal of a post-incident review should be to?

CISM Exam Overview - Vinsys

CISM Review Manual, Chapter 4, page 176

CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

Question: 194

Which of the following is the PRIMARY objective of incident triage?

A. Coordination of communications
B. Mitigation of vulnerabilities
C. Categorization of events
D. Containment of threats

Answer: C

Explanation:

The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign

the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization's information security. Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization's assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident. Reference = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; Critical Incident Stress Management - National Interagency Fire Center3; Critical Incident Stress Management - US Forest Service4

Question: 195

A financial company executive is concerned about recently increasing cyberattacks and needs to take

action to reduce risk. The organization would BEST respond by:

A. increasing budget and staffing levels for the incident response team.
B. implementing an intrusion detection system (IDS).
C. revalidating and mitigating risks to an acceptable level.
D. testing the business continuity plan (BCP).

Answer: C

Explanation:

The best response for the organization to reduce risk from increasing cyberattacks is to revalidate and mitigate risks to an acceptable level. This means that the organization should review its current risk profile, identify any new or emerging threats, vulnerabilities, or impacts, and evaluate the effectiveness of its existing controls and countermeasures. Based on this analysis, the organization should implement appropriate risk treatment strategies, such as avoiding, transferring, accepting, or reducing the risks, to achieve its desired risk appetite and tolerance. The organization should also monitor and review the risk situation and the implemented controls on a regular basis, and update its risk management plan accordingly. This approach is consistent with the ISACA Risk IT Framework, which provides guidance on how to align IT risk management with business objectives and value12. The other options are not the best responses because they are either too narrow or too reactive. Increasing budget and staffing levels for the incident response team may improve the organization's ability to respond to and recover from cyberattacks, but it does not address the root causes or the prevention of the attacks. Implementing an intrusion detection system (IDS) may enhance the organization's detection and analysis capabilities, but it does not guarantee the protection or mitigation of the attacks. Testing the business continuity plan (BCP) may verify the organization's readiness and resilience to continue its critical operations in the event of a cyberattack, but it does not reduce the likelihood or the impact of the attack. Reference = Risk IT Framework 1

CISM Review Manual, 16th Edition | Print | English 2, Chapter 3: Information Risk Management, pages 97-

98, 103-104, 107-108, 111-112.

Question: 196

An organization's HR department requires that employee account privileges be removed from all corporate IT systems within three days of termination to comply with a government regulation However, the systems all have different user directories, and it currently takes up to four weeks to remove the privileges Which of the following would BEST enable regulatory compliance?

A. Multi-factor authentication (MFA) system
B. Identity and access management (IAM) system
C. Privileged access management (PAM) system
D. Governance, risk, and compliance (GRC) system

Answer: B

Explanation:

= An identity and access management (IAM) system is a set of processes, policies, and technologies that enable an organization to manage the identities and access rights of its users across different systems and applications1. An IAM system can help an organization to comply with the government regulation by automating the provisioning and deprovisioning of user accounts, enforcing consistent access policies, and integrating different user directories2. An IAM system can also provide audit trails and reports to demonstrate compliance with the regulation3. A multi-factor authentication (MFA) system is a method of verifying the identity of a user by requiring two or more factors, such as something the user knows, has, or is4. An MFA system can enhance the security of user authentication, but it does not address the issue of removing user privileges from different systems within three days of termination. A privileged access management (PAM) system is a solution that manages and monitors the access of privileged users, such as administrators, to critical systems and resources. A PAM system can reduce the risk of unauthorized or malicious use of privileged accounts, but it does not solve the problem of managing the access of regular users across different systems. A governance, risk, and compliance (GRC) system is a software platform that integrates the functions of governance, risk management, and compliance management. A GRC system can help an organization to align its objectives, policies, and processes with the relevant regulations, standards, and best practices, but it does not directly enable the removal of user privileges from different systems within three days of termination. Reference = 1: CISM Review Manual (Digital Version), page 24 2: 1 3: 2 4: CISM Review Manual (Digital Version), page 25 : CISM Review Manual (Digital Version), page 26 : CISM Review Manual (Digital Version), page 27

Question: 197

Which of the following is MOST important to convey to employees in building a security risk-aware culture?

A. Personal information requires different security controls than sensitive information.
B. Employee access should be based on the principle of least privilege.
C. Understanding an information asset's value is critical to risk management.
D. The responsibility for security rests with all employees.

Answer: D

Explanation:

= The most important message to convey to employees in building a security risk-aware culture is that the responsibility for security rests with all employees, not just the information security function or the management. A security risk-aware culture is a collective mindset of the people in the organization working every day to protect the enterprise and its information assets from internal and external threats. A security risk-aware culture requires the workforce to know the security risks and the processes for avoiding or mitigating them, and to make thoughtful decisions that align with security policies and standards. A security risk-aware culture also incorporates a broader corporate

culture of day-to-day actions that encourage employees to report security incidents, share security best practices, and participate in security awareness and training programs. A security risk-aware culture helps to reduce the human factor that causes 90 percent of all cyberattacks, and to offset the impact of corrupted or lost data, decreased revenue, regulatory fines, and reputational damage. A security risk-aware culture turns people from assets that must be protected into assets that actively contribute to the cybersecurity and risk management posture and elevate security to being a business enabler rather than a business impediment123.

Personal information requires different security controls than sensitive information is a true statement, but it is not the most important message to convey to employees in building a security risk-aware culture. Personal information is any information that can identify or relate to a natural person, such as name, address, email, phone number, social security number, etc. Sensitive information is any information that is confidential, proprietary, or has a high value or impact to the organization, such as trade secrets, financial data, customer data, intellectual property, etc. Different types of information may have different legal, regulatory, contractual, or ethical obligations to protect them from unauthorized access, use, disclosure, modification, or destruction. Therefore, different security controls may be applied to personal and sensitive information based on their classification, such as encryption, access control, retention, disposal, etc. However, this message does not address the broader concept of security risk-aware culture, which is not limited to information classification and protection, but also encompasses the behaviors, attitudes, and values of the employees towards security.

Employee access should be based on the principle of least privilege is a good practice, but it is not the most important message to convey to employees in building a security risk-aware culture. The principle of least privilege states that users should only have the minimum level of access and permissions that are necessary to perform their job functions, and no more. This principle helps to reduce the risk of unauthorized or inappropriate actions, such as data leakage, fraud, sabotage, etc., by limiting the exposure and impact of user activities. However, this message does not capture the essence of security risk-aware culture, which is not only about access control, but also about the awareness, understanding, and commitment of the employees to security.

Understanding an information asset's value is critical to risk management is a valid point, but it is not the most important message to convey to employees in building a security risk-aware culture. Understanding an information asset's value is essential to determine the potential impact and likelihood of a security risk, and to prioritize the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance. However, this message does not reflect the holistic nature of security risk-aware culture, which is not only about risk assessment, but also about risk communication, risk treatment, and risk monitoring.

Reference = Building a Culture of Security - ISACA2

The Risk-Conscious, Security-Aware Culture: The Forgotten Critical Security Control - Cisco3 CISM ITEM DEVELOPMENT GUIDE - ISACA4

Question: 198

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

A. rely on senior management to enforce security.
B. promote the relevance and contribution of security.
C. focus on compliance.
D. reiterate the necessity of security.

Answer: B

Explanation:

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security to the organization's goals and objectives. Security is not only a technical function, but also a business enabler that supports the organization's strategy, vision, and mission. By promoting the relevance and contribution of security, the information security manager can demonstrate the value and benefits of security to the stakeholders, such as increasing customer trust, enhancing reputation, reducing costs, improving efficiency, and complying with regulations. Promoting the relevance and contribution of security can also help the information security manager to build relationships and partnerships with the business units, and to align the security program with the business needs and expectations. Promoting the relevance and contribution of security can also help the information security manager to foster a positive security culture and awareness within the organization, and to encourage the adoption and support of security policies and practices.

The other options are not the best ways to overcome the perception that security is a hindrance to business activities. Relying on senior management to enforce security is not the best way, because it may create a sense of coercion and resentment among the employees, and may undermine the credibility and authority of the information security manager. Focusing on compliance is not the best way, because it may create a false sense of security and satisfaction, and may neglect the other aspects and dimensions of security, such as risk management, value creation, and innovation.

Reiterating the necessity of security is not the best way, because it may not address the root causes and factors of the negative perception, and may not provide sufficient evidence and justification for the security investments and decisions. Reference = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 13-14, 23-241; CISM Online Review Course, Domain 1: Information Security Governance, Module 1: Information Security Governance Overview, ISACA2

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security. By demonstrating the value that security brings to the organization, including protecting assets and supporting business objectives, the information security manager can help to change the perception of security from a hindrance to a critical component of business success.

Relying on senior management to enforce security, focusing on compliance, and reiterating the necessity of security are all important elements of a comprehensive security program, but they do not directly address the perception that security is a hindrance to business activities. By promoting the relevance and contribution of security, the information security manager can help to align security with the overall goals and objectives of the organization, and foster a culture that values and supports security initiatives.

Question: 199

A risk assessment exercise has identified the threat of a denial of service (DoS) attack Executive management has decided to take no further action related to this risk. The MO ST likely reason for this decision is

A. the risk assessment has not defined the likelihood of occurrence
B. the reported vulnerability has not been validated
C. executive management is not aware of the impact potential
D. the cost of implementing controls exceeds the potential financial losses.

Answer: D

Explanation:

The most likely reason for executive management to take no further action related to the risk of a denial of service (DoS) attack is that the cost of implementing controls exceeds the potential financial losses. This means that the risk is acceptable or tolerable for the organization, and that the benefits of reducing the risk do not outweigh the costs of applying the controls. This decision is based on a cost-benefit analysis, which is a common technique for evaluating and comparing different risk response options. A cost-benefit analysis considers the following factors:

The estimated impact of the risk, which is the potential loss or damage that the organization may suffer if the risk materializes. The impact can be expressed in quantitative or qualitative terms, such as monetary value, reputation, customer satisfaction, legal liability, etc.

The estimated likelihood of occurrence, which is the probability or frequency that the risk will occur within a given time period. The likelihood can be expressed in numerical or descriptive terms, such as percentage, rating, high, medium, low, etc.

The estimated cost of controls, which is the total amount of resources that the organization needs to invest in order to implement and maintain the controls. The cost can include direct and indirect expenses, such as hardware, software, personnel, training, maintenance, etc.

The estimated benefit of controls, which is the reduction in the impact or likelihood of the risk as a result of implementing the controls. The benefit can be expressed in the same terms as the impact or likelihood, such as monetary value, percentage, rating, etc.

A cost-benefit analysis can be performed using various methods, such as net present value (NPV), return on investment (ROI), internal rate of return (IRR), etc. The general principle is to compare the cost and benefit of each control option, and select the one that provides the highest net benefit or the lowest net cost. A control option is considered feasible and desirable if its benefit exceeds its cost, or if its cost is lower than the impact of the risk.

In this case, executive management has decided to take no further action related to the risk of a DoS attack, which implies that the cost of implementing controls exceeds the potential financial losses. This could be because the impact or likelihood of the risk is low, or because the cost or complexity of the controls is high, or both. For example, the organization may have a robust backup and recovery system, a diversified network infrastructure, a strong customer loyalty, or a low dependency on online services, which reduce the impact or likelihood of a DoS attack. Alternatively, the organization may face technical, financial, or operational challenges in implementing effective controls, such as firewalls, load balancers, traffic filters, or cloud services, which increase the cost or complexity of the controls. Therefore, executive management may have concluded that the risk is acceptable or tolerable, and that taking no further action is the most rational and economical choice.

The other options are not the most likely reasons for executive management to take no further action related to the risk of a DoS attack, as they indicate a lack of proper risk assessment or validation. The risk assessment should define the likelihood of occurrence and the reported vulnerability should be validated, as these are essential steps for identifying and analyzing the risk. Executive management should be aware of the impact potential, as this is a key factor for evaluating and prioritizing the risk. If any of these options were true, executive management would not have enough information or evidence to make an informed and justified decision about the risk response. Reference = CISM Review Manual, Chapter 2, pages 67-69

CISM Exam Content Outline | CISM Certification | ISACA, Domain 2, Task 2.2

Information Security Risk Management for CISM® - Pluralsight, Module 2, Section 2.3

CISM: Information Risk Management Part 2 from Skillsoft - NICCS, Section 2.4

Executive management may not take action related to a risk if they have determined that the cost of implementing necessary controls to mitigate the risk exceeds the potential financial losses that the organization may incur if the risk were to materialize. In cases such as this, it is important for the information security team to provide the executive team with thorough cost-benefit analysis that outlines the cost of implementing the controls versus the expected losses from the risk.

Question: 200

Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?

A. Impact on information security program
B. Cost of controls
C. Impact to business function
D. Cost to replace

Answer: C

Explanation:

The level of protection for an information asset should be based on the impact to the business function that depends on the asset. The impact to the business function reflects the value and criticality of the information asset to the organization, and the potential consequences of its loss, compromise, or unavailability. The impact to the business function can be measured in terms of financial, operational, reputational, legal, or strategic effects. The higher the impact, the higher the level of protection required.

Impact on information security program, cost of controls, and cost to replace are not the best factors to provide guidance when deciding the level of protection for an information asset. Impact on information security program is a secondary effect that depends on the impact to the business function. Cost of controls and cost to replace are important considerations for implementing and maintaining the protection, but they do not determine the level of protection needed. Cost of controls and cost to replace should be balanced with the impact to the business function and the risk appetite of the organization. Reference = CISM Certified Information Security Manager Study Guide, Chapter 2: Information Risk Management, page 671; CISM Foundations: Module 2 Course, Part One: Information Risk Management2; CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, page 693

When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture. Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

Question: 201

Which of the following is the MOST effective way to demonstrate alignment of information security strategy with business objectives?

A. Balanced scorecard
B. Risk matrix
C. Benchmarking
D. Heat map

Answer: A

Explanation:

The most effective way to demonstrate alignment of information security strategy with business objectives is to use a balanced scorecard. A balanced scorecard is a strategic management tool that translates the vision and mission of an organization into a set of performance indicators that measure its progress towards its goals. A balanced scorecard typically includes four perspectives: financial, customer, internal process, and learning and growth. Each perspective has a set of objectives, measures, targets, and initiatives that are aligned with the organization's strategy. A balanced scorecard helps to communicate, monitor, and evaluate the performance of the organization and its information security program in relation to its business objectives. A balanced scorecard also helps to identify and prioritize improvement opportunities, as well as to align the activities and resources of the organization with its strategy12.

The other options are not the most effective ways to demonstrate alignment of information security strategy with business objectives. A risk matrix is a tool that displays the likelihood and impact of various risks on a two-dimensional grid. A risk matrix helps to assess and prioritize risks, as well as to determine the appropriate risk response strategies. However, a risk matrix does not show how the information security strategy supports the business objectives, nor does it measure the performance or the value of the information security program3. Benchmarking is a process of comparing the performance, practices, or processes of an organization with those of other organizations or industry standards. Benchmarking helps to identify best practices, gaps, and areas for improvement, as well as to set realistic and achievable goals. However, benchmarking does not show how the information security strategy aligns with the business objectives, nor does it reflect the unique characteristics and needs of the organization4. A heat map is a graphical representation of data using colors to indicate the intensity or frequency of a variable. A heat map can be used to visualize the distribution, concentration, or variation of risks, controls, or incidents across different dimensions, such as business units, processes, or assets. A heat map helps to highlight the areas of high risk or low control effectiveness, as well as to facilitate decision making and resource allocation. However, a heat map does not show how the information security strategy contributes to the business objectives, nor does it measure the outcomes or the benefits of the information security program5. Reference =

CISM Review Manual, 16th Edition | Print | English 2, Chapter 1: Information Security Governance, pages 28-29, 31-32, 34-35.
Balanced Scorecard - Wikipedia 1
Risk Matrix - Wikipedia 3
Benchmarking - Wikipedia 4
Heat map - Wikipedia 5

Question: 202

Which of the following is the BEST approach to make strategic information security decisions?

A. Establish regular information security status reporting.
B. Establish an information security steering committee.
C. Establish business unit security working groups.
D. Establish periodic senior management meetings.

Answer: B

Explanation:

= According to the CISM Review Manual (Digital Version), page 9, an information security steering committee is a group of senior managers from different business units and functions who provide guidance and oversight for the information security program. An information security steering committee is the best approach to make strategic information security decisions because it can: Ensure alignment of information security strategy with business objectives and risk appetite1 Facilitate communication and collaboration among different stakeholders and promote information security awareness and culture2
Provide direction and support for information security initiatives and projects3
Monitor and review the performance and effectiveness of the information security program4 Resolve conflicts and issues related to information security policies and practices5
Establishing regular information security status reporting, business unit security working groups, and periodic senior management meetings are useful activities for information security management, but they are not sufficient to make strategic information security decisions without the involvement and guidance of an information security steering committee. Reference = 1: CISM Review Manual (Digital Version), page 9 2: 1 3: 2 4: 3 5: 4

An Information Security Steering Committee is a group of stakeholders responsible for providing governance and guidance to the organization on all matters related to information security. The committee provides oversight and guidance on security policies, strategies, and technology implementation. It also ensures that the organization is in compliance with relevant laws and regulations. Additionally, it serves as a forum for discussing security-related issues and ensures that security is taken into account when making strategic decisions.

Question: 203

Which of the following is the BEST way to obtain support for a new organization-wide information security program?

A. Benchmark against similar industry organizations
B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.
D. Establish an information security strategy committee.

Answer: D

Explanation:

= Establishing an information security strategy committee is the best way to obtain support for a new organization-wide information security program because it involves the participation and collaboration of key stakeholders from different business functions and levels who can provide input, guidance, and endorsement for the security program. An information security strategy committee is a governance body that oversees the development, implementation, and maintenance of the security program and aligns it with the organization's strategic objectives, risk appetite, and culture. An information security strategy committee can help to obtain support for the security program by: Communicating the vision, mission, and goals of the security program to the organization and demonstrating its value and benefits.

Establishing roles and responsibilities for the security program and ensuring accountability and ownership.

Securing adequate resources and budget for the security program and allocating them appropriately. Resolving conflicts and issues that may arise during the security program execution and ensuring alignment with other business processes and initiatives.

Monitoring and evaluating the performance and effectiveness of the security program and ensuring continuous improvement and adaptation.

Benchmarking against similar industry organizations is a useful technique to compare and improve the security program, but it is not the best way to obtain support for a new organization-wide information security program. Benchmarking involves measuring and analyzing the security program's processes, practices, and outcomes against those of other organizations that have similar characteristics, objectives, or challenges. Benchmarking can help to identify gaps, strengths, weaknesses, opportunities, and threats in the security program and to adopt best practices and standards that can enhance the security program's performance and maturity. However, benchmarking alone does not guarantee the support or acceptance of the security program by the organization, as it may not reflect the organization's specific needs, risks, or culture.

Delivering an information security awareness campaign is a vital component of the security program, but it is not the best way to obtain support for a new organization-wide information security program. An information security awareness campaign is a set of activities and initiatives that aim to educate and inform the organization's workforce and other relevant parties about the security program's policies, standards, procedures, and guidelines, as well as the security risks, threats, and incidents that may affect the organization. An information security awareness campaign can help to increase the security knowledge, skills, and behaviors of the organization's members and to foster a security risk-aware culture. However, an information security awareness campaign is not sufficient to obtain support for the security program, as it may not address the strategic, operational, or financial aspects of the security program or the expectations and interests of the different stakeholders.

Publishing an information security RACI chart is a helpful tool to define and communicate the security program's roles and responsibilities, but it is not the best way to obtain support for a new organization-wide information security program. A RACI chart is a matrix that assigns the level of involvement and accountability for each task or activity in the security program to each role or stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four possible levels of participation. A RACI chart can help to clarify the expectations, obligations, and authority of each role or stakeholder in the security program and to avoid duplication, confusion, or conflict. However, a RACI chart does not ensure the support or

commitment of the roles or stakeholders for the security program, as it may not address the benefits, challenges, or resources of the security program or the feedback and input of the roles or stakeholders.
Reference =
CISM Review Manual 15th Edition, pages 97-98, 103-104, 107-108, 111-112
Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition - ISACA1
Information Security Strategy: The Key to Success - ISACA2

Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

Question: 204

Which of the following roles is BEST able to influence the security culture within an organization?

A. Chief information security officer (CISO)
B. Chief information officer (CIO)
C. Chief executive officer (CEO)
D. Chief operating officer (COO)

Answer: C

Explanation:

The CEO is the best able to influence the security culture within an organization because the CEO sets the tone and direction for the organization and has the authority and responsibility to ensure that the organization's objectives are aligned with its strategy. The CEO can also communicate the importance and value of information security to all stakeholders and foster a culture of security awareness and accountability. The CISO, CIO and COO are important roles in information security management, but they do not have the same level of influence and authority as the CEO. Reference = CISM Review Manual, 16th Edition, page 221; CISM Exam Content Outline, Domain 1, Task 12 The Chief Information Security Officer (CISO) is responsible for leading and coordinating an organization's information security program, and as such, is in a prime position to influence the security culture within the organization. The CISO is responsible for setting policies and standards, educating employees about security risks and best practices, and ensuring that the organization is taking appropriate measures to mitigate security risks. By demonstrating a strong commitment to
information security, the CISO can help to create a security-aware culture within the organization.

Question: 205

Which of the following backup methods requires the MOST time to restore data for an application?

A. Full backup

B. Incremental
C. Differential
D. Disk mirroring

Answer: A

Explanation:

= An incremental backup method only backs up the data that has changed since the last backup, whether it was a full or an incremental backup. This method requires the least amount of time and storage space for backup, but it requires the most time to restore data for an application. To restore data from an incremental backup, the latest full backup and all the subsequent incremental backups are needed. A full backup method backs up all the data in a system or an application at a point in time. This method requires the most amount of time and storage space for backup, but it requires the least time to restore data for an application. To restore data from a full backup, only the latest full backup is needed. A differential backup method backs up the data that has changed since the last full backup. This method requires more time and storage space for backup than the incremental method, but less than the full backup method. It also requires less time to restore data for an application than the incremental method, but more than the full backup method. To restore data from a differential backup, the latest full backup and the latest differential backup are needed. A disk mirroring method creates an exact copy of a disk on another disk in real time. This method provides the highest level of availability and fault tolerance, but it also requires twice the amount of disk space. To restore data from a disk mirroring method, the mirrored disk can be used as the primary disk in case of a failure. Reference = CISM Review Manual 15th Edition, page 201-202.
The method that requires the MOST time to restore data for an application is a Full Backup. Full backups contain all the data that is required to restore an application, but the process of restoring the data is the most time-consuming as it involves copying all the data from the backup to the application. Incremental backups only backup the changes made since the last backup, differential backups only backup changes made since the last full backup, and disk mirroring provides real-time data replication, so the data is immediately available.

Question: 206

The PRIMARY purpose for continuous monitoring of security controls is to ensure:

A. control gaps are minimized.
B. system availability.
C. effectiveness of controls.
D. alignment with compliance requirements.

Answer: C

Explanation:

The primary purpose for continuous monitoring of security controls is to ensure the effectiveness of controls. This involves regularly assessing the controls to ensure that they are meeting their intended objectives, and that any potential weaknesses are identified and addressed. Continuous monitoring also helps to ensure that control gaps are minimized, and that systems are available and aligned with compliance requirements.

The primary purpose of continuous monitoring of security controls is to ensure that the controls are operating effectively and providing adequate protection for the information assets. Continuous monitoring can also help to identify control gaps, ensure system availability, and support compliance requirements, but these are secondary benefits12 Reference = 1: SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, page 1-12: A Practical Approach to Continuous Control Monitoring, ISACA Journal, Volume 2, 2015, page 1.

Question: 207

Which of the following is the GREATEST value provided by a security information and event management (SIEM) system?

A. Maintaining a repository base of security policies
B. Measuring impact of exploits on business processes
C. Facilitating the monitoring of risk occurrences
D. Redirecting event logs to an alternate location for business continuity plan

Answer: C

Explanation:

A security information and event management (SIEM) system is a tool that collects, analyzes, and correlates security events from various sources, such as firewalls, intrusion detection systems, antivirus software, and other devices. A SIEM system can provide real-time alerts, dashboards, reports, and forensic analysis of security incidents. The greatest value of a SIEM system is that it can facilitate the monitoring of risk occurrences by identifying anomalies, trends, patterns, and indicators of compromise that may otherwise go unnoticed. A SIEM system can also help with incident response, compliance, and audit activities by providing evidence and documentation of security events.
Reference =
ISACA, CISM Review Manual, 16th Edition, 2020, page 2291
ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2082

The greatest value provided by a Security Information and Event Management (SIEM) system is

facilitating the monitoring of risk occurrences. SIEM systems collect, analyze and alert on security- related data from various sources such as firewall logs, intrusion detection/prevention systems, and system logs. This allows organizations to identify security threats in real-time and respond quickly, helping to mitigate potential harm to their systems and data.

Question: 208

An organization's quality process can BEST support security management by providing:

A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.

D. a repository for security systems documentation.

Answer: B

Explanation:

= A quality process is a set of activities that ensures that the products or services delivered by an organization meet the customer's expectations and comply with the applicable standards and regulations. A quality process can support security management by providing assurance that security requirements are met throughout the development, implementation and maintenance of information systems and processes. A quality process can also help to identify and correct security defects, measure security performance and effectiveness, and improve security practices and procedures. Reference = CISM Review Manual, 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database, question ID 2092.

An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

Question: 209

When performing a business impact analysis (BIA), who should be responsible for determining the initial recovery time objective (RTO)?

A. External consultant
B. Information owners
C. Information security manager
D. Business continuity coordinator

Answer: B

Explanation:

Information owners are responsible for determining the initial recovery time objective (RTO) for their information assets and processes, as they are the ones who understand the business requirements and impact of a disruption. An external consultant may assist in conducting the business impact analysis (BIA), but does not have the authority to decide the RTO. An information security manager may provide input on the security aspects of the RTO, but does not have the business perspective to determine the RTO. A business continuity coordinator may facilitate the BIA process and ensure the alignment of the RTO with the business continuity plan, but does not have the ownership of the information assets and processes. Reference = CISM Review Manual 15th Edition, page 202.

When performing a business impact analysis (BIA), it is the responsibility of the business continuity coordinator to determine the initial recovery time objective (RTO). The RTO is a critical component of the BIA and should be determined in cooperation with the information owners. The RTO should reflect the maximum tolerable period of disruption (MTPD) and should be used to guide the development of the recovery strategy.

Question: 210

An information security manager has been notified about a compromised endpoint device Which of the following is the BEST course of action to prevent further damage?

A. Wipe and reset the endpoint device.
B. Isolate the endpoint device.
C. Power off the endpoint device.
D. Run a virus scan on the endpoint device.

Answer: B

Explanation:

A compromised endpoint device is a potential threat to the security of the network and the data stored on it. The best course of action to prevent further damage is to isolate the endpoint device from the network and other devices, so that the attacker cannot access or spread to other systems. Isolating the endpoint device also allows the information security manager to investigate the incident and determine the root cause, the extent of the compromise, and the appropriate remediation steps. Wiping and resetting the endpoint device may not be feasible or desirable, as it may result in data loss or evidence destruction. Powering off the endpoint device may not stop the attack, as the attacker may have installed persistent malware or backdoors that can resume once the device is powered on again. Running a virus scan on the endpoint device may not be effective, as the attacker may have used sophisticated techniques to evade detection or disable the antivirus software.
Reference = CISM Review Manual, 15th Edition, page 1741; CISM Review Questions, Answers & Explanations Database, question ID 2112; Using EDR to Address Unmanaged Devices - ISACA3; Boosting Cyberresilience for Critical Enterprise IT Systems With COBIT and NIST Cybersecurity Frameworks - ISACA; Endpoint Security: On the Frontline of Cyber Risk.
The best way to reduce the risk associated with a bring your own device (BYOD) program is to implement a mobile device policy and standard. This policy should include guidelines and rules regarding the use of mobile devices, such as acceptable use guidelines and restrictions on the types of data that can be stored or accessed on the device. Additionally, it should also include

requirements for secure mobile device practices, such as the use of strong passwords, encryption, and regular patching. A mobile device management (MDM) solution can also be implemented to help ensure mobile devices meet the organizational security requirements. However, it is not enough to simply implement the policy and MDM solution; employees must also be trained on the secure mobile device practices to ensure the policy is followed.

Question: 211

An intrusion has been detected and contained. Which of the following steps represents the BEST practice for ensuring the integrity of the recovered system?

A. Install the OS, patches, and application from the original source.
B. Restore the OS, patches, and application from a backup.
C. Restore the application and data from a forensic copy.
D. Remove all signs of the intrusion from the OS and application.

Answer: A

Explanation:

After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of the recovered system is to install the OS, patches, and application from the original source, such as the vendor's website or media. This way, any malicious code or backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.

Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, page 2401

ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2132

The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

Question: 212

The PRIMARY reason to create and externally store the disk hash value when performing forensic data acquisition from a hard disk is to:

A. validate the confidentiality during analysis.
B. reinstate original data when accidental changes occur.
C. validate the integrity during analysis.
D. provide backup in case of media failure.

Answer: C

Explanation:

The disk hash value is a unique identifier that is calculated from the binary data of the disk. It is used to verify that the disk image is an exact copy of the original disk and that no changes have occurred during the acquisition or analysis process. The disk hash value is stored externally, such as on a CD- ROM or a USB drive, to prevent tampering or corruption. The disk hash value can also be used as evidence in court to prove the authenticity and reliability of the digital evidence123 Reference = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 2532: Guide to Computer Forensics and Investigations Fourth Edition, page 4-103: Forensic disk acquisition over the network, Andrea Fortuna, 2018.

The main purpose of creating and storing an external disk hash value when performing forensic data

acquisition from a hard disk is to validate the integrity of the data during the analysis. This is done by comparing the original hash value of the disk to the hash value created during the acquisition process, which can be used to ensure that the data has not been tampered with or corrupted in any way. Additionally, by creating a hash value of the disk, it can be used to quickly verify the integrity of any data that is accessed from the disk in the future.

Question: 213

Prior to conducting a forensic examination, an information security manager should:

A. boot the original hard disk on a clean system.
B. create an image of the original data on new media.
C. duplicate data from the backup media.
D. shut down and relocate the server.

Answer: B

Explanation:

= A forensic examination is a process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable. The first step in conducting a forensic examination is to create an image of the original data on new media, such as a hard disk, a CD-ROM, or a USB drive. This is done to ensure that the original data is not altered, damaged, or destroyed during the examination. An image is an exact copy of the data, including the file system, the slack space, and the deleted files. Creating an image also allows the examiner to work on a duplicate of the data, rather than the original, which may be needed as evidence in court. Booting the original hard disk on a

clean system is not a good practice, as it may change the data on the disk, such as the timestamps, the registry entries, and the log files. Duplicating data from the backup media is not sufficient, as the backup media may not contain all the data that is relevant to the investigation, such as the deleted files, the temporary files, and the swap files. Shutting down and relocating the server is not advisable, as it may cause data loss, corruption, or tampering. The server should be kept running and isolated from the network until an image is created.
Reference = CISM Review Manual 15th Edition, page 204-205.
Prior to conducting a forensic examination, an information security manager should create an image of the original data on new media. This is done in order to preserve the evidence, as making changes to the original data could potentially alter or destroy the evidence. Creating an image of the data also helps to ensure that the data remains intact and free from any interference or tampering.

Question: 214

Which of the following analyses will BEST identify the external influences to an organization's information security?

A. Business impact analysis (BIA)
B. Gap analysis
C. Threat analysis
D. Vulnerability analysis

Answer: C

Explanation:

A threat analysis will best identify the external influences to an organization's information security because it involves identifying and evaluating the sources and likelihood of potential adverse events that could affect the organization's assets, operations, or reputation. External influences include factors such as emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, and threat landscape1. A threat analysis can help the organization to align its information security strategy with its business objectives and risk appetite, and to prioritize and mitigate the most relevant and impactful threats. A business impact analysis (BIA) is a process of assessing the potential consequences of a disruption to the organization's critical business functions or processes. A BIA does not directly identify the external influences to the organization's information security, but rather the impact of those influences on the organization's continuity and recovery. A gap analysis is a process of comparing the current state of the organization's information security with a desired or expected state, based on best practices, standards, or frameworks. A gap analysis does not directly identify the external influences to the organization's information security, but rather the areas of improvement or compliance. A vulnerability analysis is a process of identifying and evaluating the weaknesses or flaws in the organization's information systems or processes that could be exploited by threats. A vulnerability analysis does not directly identify the external influences to the organization's information security, but rather the exposure or susceptibility of the organization to those influences. Reference = CISM Review Manual, 15th Edition, pages 22-232; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.113

Threat analysis is a process that is used to identify and assess the external influences or threats that

could potentially affect an organization's information security. It is used to identify potential risks and develop strategies to mitigate or reduce those risks. Threat analysis involves analyzing the environment, identifying potential threats and their potential impacts, and then evaluating the organization's current security measures and developing strategies to address any deficiencies.

Question: 215

A common drawback of email software packages that provide native encryption of messages is that the encryption:

A. cannot encrypt attachments
B. cannot interoperate across product domains.
C. has an insufficient key length.
D. has no key-recovery mechanism.

Answer: B

Explanation:

Email software packages that provide native encryption of messages use proprietary algorithms and formats that are not compatible with other email software packages. This means that the encryption cannot interoperate across product domains, and the recipients of encrypted messages must use the same email software package as the sender to decrypt and read the messages. This limits the usability and scalability of

native encryption, and may also pose security risks if the encryption algorithms or formats are not well-tested or widely accepted. A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains1234. Reference = CISM Review Manual 15th Edition, page 206. The Top 10 Email Encryption Solutions In 2023 - Expert Insights2, The Best Email Encryption Services for 2023 | PCMag3, The Top 12 Email Encryption Services for 2023 - Right Inbox4.

A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains. This means that emails sent from one product cannot be read by another product, as the encryption keys used are not compatible. This can be a problem when sending emails to people who use different software packages, as the encrypted emails cannot be read.

Question: 216

When designing a disaster recovery plan (DRP), which of the following MUST be available in order to prioritize system restoration?

A. Business impact analysis (BIA) results
B. Key performance indicators (KPIs)
C. Recovery procedures
D. Systems inventory

Answer: A

Explanation:

A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident, emergency, or threat. A BIA helps to determine the business continuity requirements and priorities for recovery of business functions and processes, including their dependencies on IT systems, applications, and data. A BIA also provides information on the financial and operational impacts of a disruption, the recovery time objectives (RTOs), the recovery point objectives (RPOs), and the minimum service levels for each business function and process. A BIA is an essential input for designing a disaster recovery plan (DRP), which is a documented and approved set of procedures and arrangements to enable an organization to respond to a disaster and resume its critical functions within a predetermined timeframe. A DRP must be based on the BIA results to ensure that the system restoration is prioritized according to the business needs and expectations. A DRP must also consider the availability and suitability of the recovery resources, such as backup systems, alternate sites, and personnel. A DRP should be tested and updated regularly to ensure its effectiveness and alignment with the changing business environment and requirements. Reference = CISM Review Manual, 15th Edition, pages 175-1761; CISM Review Questions, Answers & Explanations Database, question ID 2182; Working Toward a Managed, Mature Business Continuity Plan - ISACA3; Part Two: Business Continuity and Disaster Recovery Plans - CISM Foundations: Module 4 Course4.

A BIA is an important part of Disaster Recovery Planning (DRP). It helps identify the impact of a disruption on the organization, including the critical systems and processes that must be recovered in order to minimize that impact. The BIA results are used to prioritize system restoration and determine the resources needed to get the organization back into operation as quickly as possible.

Question: 217

Which of the following should be given the HIGHEST priority during an information security postincident review?

A. Documenting actions taken in sufficient detail
B. Updating key risk indicators (KRIs)
C. Evaluating the performance of incident response team members
D. Evaluating incident response effectiveness

Answer: D

Explanation:

An information security post-incident review is a process that aims to identify the root causes, impacts, lessons learned, and improvement actions of a security incident. The highest priority during a post-incident review should be evaluating the effectiveness of the incident response, which means assessing how well the incident response plan, procedures, roles, resources, and communication were executed and aligned with the business objectives and requirements. Evaluating the incident response effectiveness can help to identify the gaps, weaknesses, strengths, and opportunities for

improvement in the incident response process and capabilities. Documenting actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are also important activities during a post-incident review, but they are not as critical as evaluating the incident response effectiveness, which can provide a holistic and strategic view of the incident response maturity and value.

Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, page 2411

ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2192

During post-incident reviews, the highest priority should be given to evaluating the effectiveness of the incident response effort. This includes assessing the accuracy of the response to the incident, the timeliness of the response, and the efficiency of the response. It is important to assess the effectiveness of the response in order to identify areas for improvement and ensure that future responses can be more effective. Documenting the actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are all important components of a post-incident review, but evaluating incident response effectiveness should be given the highest priority.

Question: 218

The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:

A. the organization has the required funds to implement the plan.
B. compliance with legal and regulatory requirements.

C. staff participation in information security efforts.
D. the plan aligns with corporate governance.

Answer: D

Explanation:

The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly1. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization2. The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives3. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation4. Reference = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253: CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA, 2017, page 27.

Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

Question: 219

To support effective risk decision making, which of the following is MOST important to have in place?

A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls

Answer: B

Explanation:

To support effective risk decision making, it is most important to have risk reporting procedures in place. Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the

organization's structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid-level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. Reference = CISM Review Manual 15th Edition, page 207-208.

Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most

important for effective risk decision making.

Question: 220

Which of the following is the BEST tool to monitor the effectiveness of information security governance?

A. Key performance indicators (KPIs)
B. Balanced scorecard
C. Business impact analysis (BIA)
D. Risk profile

Answer: A

Explanation:

Key performance indicators (KPIs) are the best tool to monitor the effectiveness of information security governance because they are quantifiable and measurable metrics that reflect the achievement of the information security objectives and the alignment of the information security strategy with the business goals. KPIs can help to evaluate the performance, efficiency, quality, and value of the information security processes and activities, and to identify the areas of improvement or adjustment. KPIs can also provide feedback to the management and the stakeholders on the status and progress of the information security governance. Some examples of KPIs for information security governance are: percentage of compliance with security policies and standards, number and severity of security incidents, return on security investment, and maturity level of information security capabilities12.

A balanced scorecard is a strategic management tool that translates the vision and mission of the organization into four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard

can help to align the information security strategy with the business strategy, but it is not a tool to monitor the effectiveness of information security governance. A balanced scorecard can include KPIs as part of its measurement system, but it is not a substitute for KPIs13.

A business impact analysis (BIA) is a process of assessing the potential consequences of a disruption to the organization's critical business functions or processes. A BIA can help to identify the critical assets, dependencies, recovery priorities, and recovery objectives for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A BIA is a one-time or periodic activity, not a continuous monitoring process14.

A risk profile is a representation of the organization's exposure to various types of risks, such as operational, financial, strategic, or reputational. A risk profile can help to identify the sources, likelihood, and impact of potential threats to the organization's assets and objectives, and to determine the risk appetite and tolerance for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A risk profile is a snapshot of the organization's risk posture at a given point in time, not a dynamic monitoring tool15. Reference = CISM Review Manual, 16th Edition, pages 23-241; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.122; CISM Review Questions, Answers & Explanations Database, Question ID 10093; CISM Review Questions, Answers & Explanations Database, Question ID 10104; CISM Review Questions, Answers & Explanations Database, Question ID 10115

Question: 221

Which of the following has the MOST influence on the inherent risk of an information asset?

A. Risk tolerance
B. Net present value (NPV)
C. Return on investment (ROI)
D. Business criticality

Answer: D

Explanation:

Inherent risk is the risk that exists before any controls are applied. It is influenced by factors such as the nature, value, sensitivity, and exposure of the information asset. Business criticality is one of the most important factors that affect the inherent risk of an information asset, as it reflects how essential the asset is for the organization's operations and objectives. The higher the business criticality, the higher the inherent risk. Risk tolerance, NPV, and ROI are not directly related to the inherent risk of an information asset, as they are more relevant for the risk assessment and risk treatment processes. Reference = CISM Review Manual, 16th Edition, page 971

Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

Question: 222

Which of the following is the GREATEST inherent risk when performing a disaster recovery plan (DRP) test?

A. Poor documentation of results and lessons learned
B. Lack of communication to affected users
C. Disruption to the production environment
D. Lack of coordination among departments

Answer: C

Explanation:

A disaster recovery plan (DRP) test is a simulation of a disaster scenario to evaluate the effectiveness and readiness of the DRP. The greatest inherent risk when performing a DRP test is the disruption to the production environment, which could cause operational issues, data loss, or system damage. Therefore, it is essential to plan and execute the DRP test carefully, with proper backup, isolation,

and rollback procedures. Poor documentation, lack of communication, and lack of coordination are also potential risks, but they are not as severe as disrupting the production environment. Reference = CISM Review Manual 15th Edition, page 253; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 224.

The greatest inherent risk when performing a disaster recovery plan (DRP) test is disruption to the production environment. A DRP test involves simulating a disaster scenario to ensure that the organization's plans are effective and that it is able to recover from an incident. However, this involves running tests on the production environment, which has the potential to disrupt the normal operations of the organization. This inherent risk can be mitigated by running tests on a nonproduction environment or by running tests at times when disruption will be minimized.

Question: 223

Which of the following BEST determines the allocation of resources during a security incident response?

A. Senior management commitment
B. A business continuity plan (BCP)
C. An established escalation process
D. Defined levels of severity

Answer: D

Explanation:

= The allocation of resources during a security incident response depends on the defined levels of severity, which indicate the potential impact and urgency of the incident. The levels of severity help prioritize the response activities and assign the appropriate roles and responsibilities. Senior management commitment, a business continuity plan (BCP), and an established escalation process are important factors for an effective incident response, but they do not directly determine the allocation of resources. Reference = CISM Review Manual, 16th Edition, page 3011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462

Learn more:

1. isaca.org2. amazon.com3. gov.uk

Defined levels of severity is the best determinant of the allocation of resources during a security incident response. Having defined levels of severity allows organizations to plan for and allocate resources for each level of incident, depending on the severity of the incident. This ensures that the right resources are allocated in a timely manner and that incidents are addressed appropriately.

Question: 224

During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

A. baseline security controls.
B. benchmarking security metrics.
C. security objectives.
D. cost-benefit analyses.

Answer: C

Explanation:

During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address security objectives, which are derived from the business objectives and the risk assessment. Security objectives define the desired level of protection for the system and its data, and guide the selection of security controls in later phases. Baseline security controls are predefined sets of security requirements that apply to common types of systems or environments. Benchmarking security metrics is a process of comparing the performance of security processes or controls against a standard or best practice. Cost-benefit analyses are used to evaluate the feasibility and effectiveness of security controls, and are usually performed in the acquisition/development phase or the implementation phase of the SDLC. Reference = CISM Review Manual, 16th Edition, page 1021; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 772

Learn more:

1. isaca.org2. amazon.com3. gov.uk

Question: 225

Which of the following would BEST justify continued investment in an information security program?

A. Reduction in residual risk
B. Security framework alignment
C. Speed of implementation
D. Industry peer benchmarking

Answer: A

Explanation:

Residual risk is the risk that remains after implementing controls to mitigate the inherent risk. A reduction in residual risk indicates that the information security program is effective in managing the risks to an acceptable level. This would best justify the continued investment in the program, as it demonstrates the value and benefits of the security activities. Security framework alignment, speed of implementation, and industry peer benchmarking are not direct measures of the effectiveness or value of the information security program. They may be useful for comparison or compliance purposes, but they do not necessarily reflect the impact of the program on the risk profile of the organization. Reference = CISM Review Manual, 16th Edition, page 431; CISM Review Questions,

Answers & Explanations Manual, 10th Edition, page 622

Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

Question: 226

An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?

A. Include security requirements in the contract
B. Assess security controls.
C. Perform a risk assessment
D. Review data architecture.

Answer: C

Explanation:

Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app

The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

Question: 227

Which of the following sources is MOST useful when planning a business-aligned information security program?

A. Security risk register
B. Information security policy
C. Business impact analysis (BIA)
D. Enterprise architecture (EA)

Answer: C

Explanation:

A business-aligned information security program is one that supports the organization's business objectives and aligns the information security strategy with the business functions. A business impact analysis (BIA) is a process that identifies the critical business processes, assets, and functions of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA helps to prioritize the information security requirements and controls that are needed to protect the organization's critical assets and functions from various threats and risks. Therefore, a BIA is one of the most useful sources when planning a business-aligned information security program. Reference = CISM Review Manual 15th Edition, page 254; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 229.

The most useful source when planning a business-aligned information security program is a Business Impact Analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to an organization's operations, and helps to identify the security controls and measures that should be implemented to reduce the impact of those disruptions. The BIA should include an assessment of the organization's information security posture, including its security policies, risk register, and enterprise architecture. With this information, organizations can develop an information security program that is aligned to the organization's business objectives.

Question: 228

When collecting admissible evidence, which of the following is the MOST important requirement?

A. Need to know
B. Preserving audit logs
C. Due diligence
D. Chain of custody

Answer: D

Explanation:

Chain of custody is the MOST important requirement when collecting admissible evidence, because it ensures the integrity and authenticity of the evidence by documenting its history, handling, and storage. Chain of

custody records who, what, when, where, why, and how the evidence was collected, analyzed, and preserved. Without a proper chain of custody, the evidence may be challenged or rejected in a court of law. Need to know, preserving audit logs, and due diligence are important aspects of evidence collection, but they are not as critical as chain of custody. Reference = CISM Review Manual, 16th Edition, page 3031; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492

The most important requirement when collecting admissible evidence is the chain of custody. The chain of custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

Question: 229

Which of the following should be the PRIMARY basis for an information security strategy?

A. The organization's vision and mission
B. Results of a comprehensive gap analysis
C. Information security policies
D. Audit and regulatory requirements

Answer: A

Explanation:

The organization’s vision and mission should be the PRIMARY basis for an information security strategy, as they define the purpose and direction of the organization and its information security needs. A comprehensive gap analysis is a tool to identify the current state and desired state of information security, and the actions needed to close the gap. Information security policies are the high-level statements of management’s intent and expectations for information security, and are derived from the information security strategy. Audit and regulatory requirements are external factors that influence the information security strategy, but are not the primary basis for it. Reference = CISM Review Manual, 16th Edition, pages 17-181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 782

The primary basis for an information security strategy should be the organization's vision and mission. The organization's vision and mission should be the foundation for the security strategy, and should inform and guide the security policies, procedures, and practices that are implemented. The results of a comprehensive gap analysis, information security policies, and audit and regulatory requirements should all be taken into consideration when developing the security strategy, but should not be the primary basis.

Question: 230

An information security manager learns through a threat intelligence service that the organization may be targeted for a major emerging threat. Which of the following is the information security manager's FIRST course of action?

A. Conduct an information security audit.
B. Validate the relevance of the information.
C. Perform a gap analysis.

D. Inform senior management

Answer: B

Explanation:

The information security manager's first course of action should be to validate the relevance of the information received from the threat intelligence service. This means verifying the source, credibility, accuracy, and timeliness of the information, as well as assessing the potential impact and likelihood of the threat for the organization. This will help the information security manager to determine the appropriate response and prioritize the actions to mitigate the threat. Conducting an information security audit, performing a gap analysis, and informing senior management are possible subsequent actions, but they are not the first course of action. An information security audit is a systematic and independent assessment of the effectiveness of the information security controls and processes. A gap analysis is a comparison of the current state of the information security program with the desired state or best practices. Informing senior management is a communication activity that should be done after validating the information and assessing the risk. Reference = CISM Review Manual, 16th Edition, pages 44-451; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 632

The first step the information security manager should take upon learning of the potential threat is to validate the relevance of the information. This should involve researching the threat to evaluate its potential impact on the organization and to determine the accuracy of the threat intelligence. Once the information is validated, the information security manager can then take action, such as informing senior management, conducting an information security audit, or performing a gap analysis.

Question: 231

The PRIMARY advantage of single sign-on (SSO) is that it will:

A. increase efficiency of access management
B. increase the security of related applications.
C. strengthen user passwords.
D. support multiple authentication mechanisms.

Answer: A

Explanation:

Single sign-on (SSO) is a technology that allows users to access multiple applications or services with one set of credentials, such as a username and password. The primary advantage of SSO is that it increases the efficiency of access management, as it reduces the need for users to remember and enter multiple passwords for different applications or services. SSO also simplifies the user experience, as they can log in once and access multiple resources without having to switch between different windows or tabs. SSO can also improve the security of related applications, as it reduces the risk of password compromise or phishing attacks. However, SSO does not strengthen user passwords or support multiple authentication mechanisms by itself. It is a complementary technology that enhances the security and convenience of access management. Reference = CISM Review Manual, 16th Edition, page 991

The primary advantage of single sign-on (SSO) is that it increases the efficiency of access

management. With SSO, users only need to remember one set of credentials to access all of their applications, rather than having to remember multiple usernames and passwords for each application. This simplifies the user experience and helps to reduce the amount of time spent managing access to multiple applications. Additionally, SSO can also increase the security of related applications, as users are not sharing the same credentials across multiple applications, and it can also support multiple authentication mechanisms, such as biometric authentication.

Question: 232

A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. The chief information security officer (CISO) should be MOST concerned with:

A. developing a security program that meets global and regional requirements.
B. ensuring effective communication with local regulatory bodies.
C. using industry best practice to meet local legal regulatory requirements.
D. monitoring compliance with defined security policies and standards.

Answer: A

Explanation:

= A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. This means that the CISO has to deal with multiple and diverse legal, regulatory, and compliance issues across different jurisdictions and markets. The CISO should be most concerned with developing a security program that meets global and regional requirements, such as ISO/IEC 27001, NIST CSF, PCI DSS, GDPR, etc. These standards provide a framework for establishing, implementing, maintaining, and improving an information security management system (ISMS) that aligns with the organization's business objectives and risk appetite. The CISO should also ensure that the security program is consistent and coherent across all operating locations, and that it complies with the specific regulations of each location. Therefore, option A is the most appropriate answer. Reference = CISM Review Manual 15th Edition, page 255; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 234.
In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

Question: 233

The PRIMARY objective of performing a post-incident review is to:

A. re-evaluate the impact of incidents
B. identify vulnerabilities

C. identify control improvements.
D. identify the root cause.

Answer: D

Explanation:

= The PRIMARY objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled the incident to occur. Identifying the root cause helps to prevent or mitigate future incidents, as well as to improve the incident response process. Re-evaluating the impact of incidents, identifying vulnerabilities, and identifying control improvements are secondary objectives of a post-incident review, which are derived from the root cause analysis. Reference = CISM Review Manual, 16th Edition, page 3061; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1512

The primary objective of performing a post-incident review is to identify the root cause of the incident. After an incident has occurred, the post-incident review process involves gathering and analyzing evidence to determine the cause of the incident. This analysis will help to identify both the underlying vulnerability that allowed the incident to occur, as well as any control improvements that should be implemented to prevent similar incidents from occurring in the future. Additionally, the post-incident review process can also be used to re-evaluate the impact of the incident, as well as any potential implications for the organization.

Question: 234

Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?

A. Legal and regulatory requirements
B. Likelihood of a disaster
C. Organizational tolerance to service interruption
D. Geographical location of the backup site

Answer: C

Explanation:

= The organizational tolerance to service interruption is the most important consideration when defining a recovery strategy in a business continuity plan (BCP), as it reflects the degree of risk that the organization is willing to accept in the event of a disaster. The organizational tolerance to service interruption determines the acceptable level of downtime, data loss, or disruption that the organization can tolerate, and thus guides the selection of recovery objectives, strategies, and resources. Legal and regulatory requirements are external factors that influence the recovery strategy, but are not the primary consideration. Likelihood of a disaster is a factor that affects the

recovery strategy, but is not the most important one. Geographical location of the backup site is a factor that affects the recovery strategy, but is not as critical as organizational tolerance to service interruption. Reference = CISM Review Manual, 16th Edition, page 1731; CISM Review Questions, Answers & Explanations

Manual, 10th Edition, page 792

Learn more:

1. isaca.org2. amazon.com3. gov.uk

Question: 235

The fundamental purpose of establishing security metrics is to:

A. increase return on investment (ROI)
B. provide feedback on control effectiveness
C. adopt security best practices
D. establish security benchmarks

Answer: B

Explanation:

The fundamental purpose of establishing security metrics is to provide feedback on the effectiveness of the information security controls and processes. Security metrics are quantitative or qualitative measures that indicate how well the organization is achieving its security objectives and goals. Security metrics can help the information security manager to monitor, evaluate, and improve the performance of the information security program, as well as to identify gaps, weaknesses, and areas for improvement. Security metrics can also help the organization to demonstrate compliance with internal and external standards, regulations, and best practices. Increasing return on investment (ROI), adopting security best practices, and establishing security benchmarks are possible outcomes or benefits of using security metrics, but they are not the fundamental purpose of establishing them. Reference = CISM Review Manual, 16th Edition, pages 46-471; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 642

Learn more:

1. isaca.org2. amazon.com3. gov.uk

Security metrics are used to measure the effectiveness of controls and evaluate the overall security posture of an organization. This feedback provides an understanding of the progress made towards achieving security objectives and allows organizations to make necessary adjustments.

Question: 236

Which of the following is the BEST approach when creating a security policy for a global organization subject to varying laws and regulations?

A. Incorporate policy statements derived from third-party standards and benchmarks.
B. Adhere to a unique corporate privacy and security standard
C. Establish baseline standards for all locations and add supplemental standards as required
D. Require that all locations comply with a generally accepted set of industry

Answer: C

Explanation:

= Creating a security policy for a global organization subject to varying laws and regulations is a challenging task, as it requires balancing the need for consistency, compliance, and flexibility. The best approach is to establish baseline standards for all locations that reflect the organization's overall security objectives, principles, and requirements. These standards should be aligned with the organization's mission, vision, values, and strategy, as well as with the applicable laws and regulations of each location. The baseline standards should also be reviewed and updated periodically to ensure their relevance and effectiveness. Additionally, supplemental standards can be added as required to address specific issues or risks that may arise in different locations or situations. Supplemental standards should be based on the best practices and lessons learned from the baseline standards, as well as on the feedback and input from the stakeholders of each location. Reference = CISM Review Manual, 16th Edition, page 1001

Question: 237

Which of the following presents the GREATEST challenge to the recovery of critical systems and data following a ransomware incident?

A. Lack of encryption for backup data in transit
B. Undefined or undocumented backup retention policies
C. Ineffective alert configurations for backup operations
D. Unavailable or corrupt data backups

Answer: D

Explanation:

A ransomware incident is a type of cyberattack that encrypts the victim's data and demands a ransom for its decryption. Ransomware can cause significant disruption and damage to critical systems and data, as well as financial losses and reputational harm. To recover from a ransomware incident, the organization needs to have reliable and accessible backups of its data, preferably in an encrypted format. However, if the backups are unavailable or corrupt, the organization will face a major challenge in restoring its data and operations. Therefore, option D is the most challenging factor for the recovery of critical systems and data following a ransomware incident. Reference = CISA MS-ISAC Ransomware Guide1, page 9; How to Write an Incident Response Plan for Ransomware Recovery2.

Question: 238

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

A. Fallback processes are tested the weekend before changes are made
B. Users are not notified of scheduled system changes
C. A manual rather than an automated process is used to compare program versions.

D. The development manager migrates programs into production

Answer: D

Explanation:

The change management procedure that is MOST likely to cause concern to the information security manager is the development manager migrating programs into production, because it involves a high-risk activity that could compromise the confidentiality, integrity, and availability of the information systems and data. Migrating programs into production without proper testing, validation, and approval could introduce errors, vulnerabilities, or conflicts that could affect the performance, functionality, or security of the systems. Fallback processes are tested the weekend before changes are made, users are not notified of scheduled system changes, and a manual rather than an automated process is used to compare program versions are all acceptable change management procedures that do not pose significant risks to the information security manager. Reference = CISM Review Manual, 16th Edition, page 3121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1522

Question: 239

Which of the following is an example of risk mitigation?

A. Purchasing insurance
B. Discontinuing the activity associated with the risk
C. Improving security controls
D. Performing a cost-benefit analysis

Answer: C

Explanation:

Improving security controls is an example of risk mitigation, which is the process of reducing the likelihood or impact of a risk. Risk mitigation can be achieved by implementing various strategies, such as purchasing insurance, discontinuing the activity associated with the risk, or improving security controls. Purchasing insurance is a form of risk transfer, which is the process of shifting the responsibility or burden of a risk to another party. Discontinuing the activity associated with the risk is a form of risk avoidance, which is the process of eliminating or avoiding a potential source of harm. Performing a cost-benefit analysis is a form of risk evaluation, which is the process of assessing the costs and benefits of different options to manage a risk. Reference = CISM Review Manual, 16th

Edition, page 1741; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 802

Question: 240

Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?

A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process

Answer: D

Explanation:

A detailed incident notification process is most important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals. The incident notification process defines the roles and responsibilities of the incident response team members, the escalation procedures, the communication channels, the reporting requirements, and the stakeholders to be informed. The incident notification process helps to ensure that the right people are involved in the incident response, that the incident is handled in a timely and efficient manner, and that the relevant information is shared with the appropriate parties. Skills required for the incident response team, a list of external resources to assist with incidents, and service level agreements (SLAs) are also important elements of an incident response plan, but they are not as critical as the incident notification process. Skills required for the incident response team describe the competencies and qualifications of the team members, but they do not specify who should be notified or involved in the incident response. A list of external resources to assist with incidents provides a directory of external parties that can provide support or expertise in the incident response, but it does not define the criteria or process for engaging them. Service level agreements (SLAs) define the expectations and obligations of the service providers and the service recipients in the incident response, but they do not detail the steps or procedures for notifying or escalating incidents. Reference = CISM Review Manual, 16th Edition, pages 191-1921; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 662

Question: 241

The PRIMARY objective of a post-incident review of an information security incident is to:

A. update the risk profile
B. minimize impact
C. prevent recurrence.
D. determine the impact

Answer: C

Explanation:

post-incident review of an information security incident is a process that aims to identify the root causes, contributing factors, and lessons learned from the incident, and to implement corrective and preventive actions to avoid or mitigate similar incidents in the future. The primary objective of a post-incident review is to prevent recurrence, as it helps to improve the security posture, awareness, and resilience of the organization. Preventing recurrence also helps to reduce the impact and cost of future incidents, as well as to enhance the reputation and trust of the organization. Updating the risk profile, minimizing impact, and determining the impact are not the primary objectives of a postincident review, although they may be part of its outcomes or

outputs. Reference = CISM Review Manual, 16th Edition, page 1011

Question: 242

While classifying information assets an information security manager notices that several production databases do not have owners assigned to them What is the BEST way to address this situation?

A. Assign responsibility to the database administrator (DBA).
B. Review the databases for sensitive content.
C. Prepare a report of the databases for senior management.
D. Assign the highest classification level to those databases.

Answer: A

Explanation:

Information asset classification is the process of identifying, labeling, and categorizing information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to establish appropriate security controls, policies, and procedures for protecting the information assets from unauthorized access, use, disclosure, modification, or destruction. One of the key elements of information asset classification is assigning owners to each information asset. Owners are responsible for managing the information asset throughout its lifecycle, including defining its security requirements, implementing security controls, monitoring its usage and performance, reporting any incidents or breaches, and ensuring compliance with legal and regulatory obligations. Therefore, assigning responsibility to the database administrator (DBA) is the best way to address the situation where several production databases do not have owners assigned to them. Reference = CISM Review Manual 15th Edition1, page 256; Information Asset and Security Classification Procedure2.

Question: 243

Which of the following events would MOST likely require a revision to the information security program?

A. An increase in industry threat level .

B. A significant increase in reported incidents
C. A change in IT management
D. A merger with another organization

Answer: D

Explanation:

= A merger with another organization would MOST likely require a revision to the information security program, because it involves a significant change in the scope, structure, and objectives of the organization. A merger could affect the information security policies, procedures, roles, responsibilities, and resources of the organization, as well as introduce new risks and challenges. Therefore, the information security program

should be reviewed and updated to reflect the new situation and ensure alignment with the organizational goals and strategies. An increase in industry threat level, a significant increase in reported incidents, and a change in IT management are all events that could affect the information security program without necessarily requiring a revision. Reference = CISM Review Manual, 16th Edition, page 3181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1532

Question: 244

Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site Which of the following issues would be of GREATEST concern to an information security manager?

A. The application does not use a secure communications protocol
B. The application is configured with restrictive access controls
C. The business process has only one level of error checking
D. Server-based malware protection is not enforced

Answer: A

Explanation:

Server-based malware protection is not enforced is the issue that would be of GREATEST concern to an information security manager, as it exposes the web-based application and its data to potential threats from malicious software that can compromise the confidentiality, integrity, and availability of the information. Server-based malware protection is a security control that monitors and blocks malicious activities on the server where the application runs, such as viruses, worms, trojans, ransomware, etc. Without server-based malware protection, the web-based application may be vulnerable to attacks that can damage or destroy the data stored on the server, or disrupt the normal functioning of the application. The other issues are also important, but not as critical as server-based malware protection. The application does not use a secure communications protocol may expose sensitive data in transit to eavesdropping or interception by unauthorized parties. The application is configured with restrictive access controls may limit the access rights of legitimate users to

authorized resources, but it does not prevent unauthorized users from accessing them through other means. The business process has only one level of error checking may result in incorrect or inconsistent data entry or processing, but it does not guarantee data quality or accuracy. Reference = CISM Review Manual, 16th Edition, page 1751; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 812

Question: 245

Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?

A. Patch management files
B. Network system logs
C. Configuration management files
D. Intrusion detection system (IDS) logs

Answer: A

Explanation:

Patch management files are the files that contain the patches or updates for the software applications and systems that are installed on the compromised system. Patch management files are essential to recover a compromised system that needs a complete rebuild, as they can help to restore the functionality, security, and performance of the system. Without patch management files, the system may not be able to run properly or securely, and may expose the organization to further risks or vulnerabilities. Network system logs, configuration management files, and intrusion detection system (IDS) logs are also important for recovering a compromised system, but they should be considered after patch management files. Network system logs can help to identify the source and scope of the attack, configuration management files can help to restore the original settings and policies of the system, and IDS logs can help to detect any malicious activities or anomalies on the system. Reference = CISM Review Manual, 16th Edition, pages 193-1941; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 672

Question: 246

Which of the following is the BEST indication that an organization has a mature information security culture?

A. Information security training is mandatory for all staff.
B. The organization's information security policy is documented and communicated.
C. The chief information security officer (CISO) regularly interacts with the board.
D. Staff consistently consider risk in making decisions.

Answer: D

Explanation:

The BEST indication that an organization has a mature information security culture is when its staff consistently consider risk in making decisions. When an organization's staff understands the risks associated with their actions and are empowered to make risk-informed decisions, it indicates that the organization has a mature information security culture.

According to the Certified Information Security Manager (CISM) Study Manual, "A mature information security culture exists when the people within the organization understand and appreciate the risks associated with information and technology and when they take steps to manage those risks on a daily basis."

While information security training, documented information security policies, and regular interaction between the chief information security officer (CISO) and the board are all important components of a mature information security culture, they are not sufficient on their own. It is only when staff consistently consider risk in making decisions that an organization's information security culture can be considered mature.

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 151-152.

Question: 247

What is the PRIMARY benefit to an organization that maintains an information security governance framework?

A. Resources are prioritized to maximize return on investment (ROI)
B. Information security guidelines are communicated across the enterprise_
C. The organization remains compliant with regulatory requirements.
D. Business risks are managed to an acceptable level.

Answer: D

Explanation:

According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.

Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization's objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.

According to the Certified Information Security Manager (CISM) Study Manual, "Information security governance provides a framework for managing and controlling information security practices and technologies at an enterprise level. Its primary objective is to manage and reduce risk through a process of identification, assessment, and management of those risks."

While the other options listed (prioritizing resources, communicating guidelines, and remaining compliant with regulations) are also important benefits of maintaining an information security governance framework, they are all secondary to the primary benefit of managing business risks to an acceptable level.

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 60-63.

Question: 248

Which of the following would be MOST effective in gaining senior management approval of security investments in network infrastructure?

A. Performing penetration tests against the network to demonstrate business vulnerability
B. Highlighting competitor performance regarding network best security practices
C. Demonstrating that targeted security controls tie to business objectives
D. Presenting comparable security implementation estimates from several vendors

Answer: C

Explanation:

The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives. Security investments should be

tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization's business objectives, senior management will be more likely to approve the investment.

According to the Certified Information Security Manager (CISM) Study Manual, "To gain senior management's approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization."

While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization's business objectives.

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 305.

Question: 249

Which of the following should be the PRIMARY objective of an information security governance framework?

A. Provide a baseline for optimizing the security profile of the organization.
B. Demonstrate senior management commitment.
C. Demonstrate compliance with industry best practices to external stakeholders.
D. Ensure that users comply with the organization's information security policies.

Answer: A

Explanation:

According to the Certified Information Security Manager (CISM) Study Manual, "The primary objective of information security governance is to provide a framework for managing and controlling information security practices and technologies at an enterprise level. Its goal is to manage and reduce risk through a process of identification, assessment, and management of those risks." While demonstrating senior management commitment, compliance with industry best practices, and ensuring user compliance with policies are all important aspects of information security governance, they are not the primary objective. The primary objective is to manage and reduce risk by establishing a framework for managing and controlling information security practices and technologies at an enterprise level.

Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 60.

Question: 250

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

A. Determine recovery priorities.
B. Define the recovery point objective (RPO).
C. Confirm control effectiveness.
D. Analyze vulnerabilities.

Answer: A

Explanation:

The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans. Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

Question: 251

Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?

A. Providing training from third-party forensics firms
B. Obtaining industry certifications for the response team
C. Conducting tabletop exercises appropriate for the organization
D. Documenting multiple scenarios for the organization and response steps

Answer: C

Explanation:

The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.
Tabletop exercises are an effective way to test and validate an organization's incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.
According to the Certified Information Security Manager (CISM) Study Manual, "Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan."
While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 324.

Question: 252

Which of the following should an information security manager do FIRST when a mandatory security standard hinders the achievement of an identified business objective?

A. Revisit the business objective.
B. Escalate to senior management.

C. Perform a cost-benefit analysis.
D. Recommend risk acceptance.

Answer: B

Explanation:

Escalate to senior management, because this could help the information security manager to inform the decision-makers of the situation, explain the implications and trade-offs, and seek their guidance and approval for the next steps2. However, this answer is not certain, and you might need to consider other factors as well.

Question: 253

Which of the following is the MOST important detail to capture in an organization's risk register?

A. Risk appetite
B. Risk severity level
C. Risk acceptance criteria
D. Risk ownership

Answer: D

Explanation:

Risk ownership is the most important detail to capture in an organization's risk register. Risk ownership is the responsibility for managing a risk, including taking corrective action, and should be assigned to a specific individual or team. It is important to note that the risk owner is not necessarily the same as the risk acceptor, who is the individual or team who makes the final decision to accept a risk. Capturing risk ownership in the risk register is important to ensure that risks are actively managed and that the responsible parties are held accountable.

Question: 254

Which of the following is the BEST reason for an organization to use Disaster Recovery as a Service (DRaaS)?

A. It transfers the risk associated with recovery to a third party.
B. It lowers the annual cost to the business.
C. It eliminates the need to maintain offsite facilities.
D. It eliminates the need for the business to perform testing.

Answer: B

Explanation:

Question: 255

Which of the following is the MOST important reason for obtaining input from risk owners when implementing controls?

A. To reduce risk mitigation costs
B. To resolve vulnerabilities in enterprise architecture (EA)
C. To manage the risk to an acceptable level
D. To eliminate threats impacting the business

Answer: C

Explanation:

According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level.
By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

Question: 256

Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?

A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats

Answer: B

Explanation:

Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

Question: 257

Which of the following is the GREATEST benefit of including incident classification criteria within an incident response plan?

A. Ability to monitor and control incident management costs
B. More visibility to the impact of disruptions
C. Effective protection of information assets
D. Optimized allocation of recovery resources

Answer: D

Explanation:

The explanation given in the manual is:
Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

Question: 258

A balanced scorecard MOST effectively enables information security:

A. risk management
B. project management
C. governance
D. performance

Answer: C

Explanation:

A balanced scorecard enables information security governance by providing a framework for aligning security objectives with business goals and measuring performance against them. The other choices are not directly related to governance but may be supported by it.
A balanced scorecard is a strategic management tool that describes the cause-and-effect linkages between four high-level perspectives of strategy and execution: financial, customer, internal process, and learning and growth2. It helps organizations communicate and monitor their vision and strategy across different levels and functions2.

Question: 259

Which of the following BEST enables an organization to provide ongoing assurance that legal and regulatory compliance requirements can be met?

A. Embedding compliance requirements within operational processes
B. Engaging external experts to provide guidance on changes in compliance requirements
C. Performing periodic audits for compliance with legal and regulatory requirements
D. Assigning the operations manager accountability for meeting compliance requirements

Answer: A

Explanation:

Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes.
Regulatory compliance involves following external legal mandates set forth by state, federal, or international government2. Compliance requirements may vary depending on the industry, location, and nature of the organization2. Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct2.

Question: 260

The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?

A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls
D. Ask the business owner for the new remediation plan

Answer: B

Explanation:

The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability. This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner. The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

Question: 261

Which of the following is the MOST critical factor for information security program success?

A. comprehensive risk assessment program for information security
B. The information security manager's knowledge of the business
C. Security staff with appropriate training and adequate resources
D. Ongoing audits and addressing open items

Answer: B

Explanation:

The explanation given in the manual is:
The information security manager's knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager's knowledge of the business.

An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations. An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture, strategy, processes, and needs of an organization to ensure that security supports its objectives.

Question: 262

Which of the following has the GREATEST influence on an organization's information security strategy?

A. The organization's risk tolerance
B. The organizational structure
C. Industry security standards
D. Information security awareness

Answer: A

Explanation:

An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives.
Therefore, an organization's risk tolerance has the greatest influence on its information security strategy.
The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security

awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance. An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security

strategy should align with the organization's business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

Question: 263

Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?

A. Security metrics
B. Security baselines
C. Security incident details
D. Security risk exposure

Answer: A

Explanation:

Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.

An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations. The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

Question: 264

Reverse lookups can be used to prevent successful:

A. denial of service (DoS) attacks
B. session hacking
C. phishing attacks
D. Internet protocol (IP) spoofing

Answer: D

Explanation:

Reverse lookups can be used to prevent successful IP spoofing. IP spoofing is a type of attack in which an attacker sends packets with a false source IP address in order to disguise their identity or impersonate another system. By performing reverse lookups on the source IP address of incoming packets, the system can verify that the packets are coming from a trusted source, and any packets with an invalid or spoofed source IP can be discarded. This is an important measure for preventing IP spoofing, and can help to reduce the risk of other types of attacks, such as DoS attacks, session hacking, and phishing attacks.

Question: 265

Which of the following is the MOST effective way to prevent information security incidents?

A. Implementing a security information and event management (SIEM) tool
B. Implementing a security awareness training program for employees
C. Deploying a consistent incident response approach
D. Deploying intrusion detection tools in the network environment

Answer: B

Explanation:

The most effective way to prevent information security incidents is to implement a security awareness training program for employees. Security awareness training provides employees with the knowledge and skills they need to identify potential security threats and protect their systems from unauthorized access and malicious activity. Security awareness training also helps to ensure that employees understand their roles and responsibilities when it comes to information security, and can help to reduce the risk of information security incidents by making employees more aware of potential risks. Additionally, implementing a security information and event management (SIEM) tool, deploying a consistent incident response approach, and deploying intrusion detection tools in the network environment can also help to reduce the risk of security incidents

Question: 266

Which of the following BEST demonstrates the added value of an information security program?

A. Security baselines
B. A gap analysis
C. A SWOT analysis
D. A balanced scorecard

Answer: D

Explanation:

A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

Question: 267

Which of the following should be the FIRST step in developing an information security strategy?

A. Determine acceptable levels of information security risk
B. Create a roadmap to identify security baselines and controls
C. Perform a gap analysis based on the current state
D. Identify key stakeholders to champion information security

Answer: D

Explanation:

The first step in developing an information security strategy is to identify key stakeholders who can provide support, guidance and resources for information security initiatives. These stakeholders may include senior management, business unit leaders, legal counsel, audit and compliance officers and other relevant parties. By engaging these stakeholders early on, an information security manager can ensure that the strategy aligns with business objectives and expectations, as well as gain buy-in and commitment from them. Determining acceptable levels of risk, creating a roadmap and performing a gap analysis are all important steps in developing an information security strategy, but they should follow after identifying key stakeholders.

Question: 268

Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

A. Risk acceptance by the business has been documented
B. Teams and individuals responsible for recovery have been identified
C. Copies of recovery and incident response plans are kept offsite
D. Incident response and recovery plans are documented in simple language

Answer: B

Explanation:

Before conducting full-functional continuity testing, an information security manager should verify

that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities. This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as

important as having clear roles and responsibilities defined before testing.

Question: 269

An anomaly-based intrusion detection system (IDS) operates by gathering data on:

A. normal network behavior and using it as a baseline lor measuring abnormal activity
B. abnormal network behavior and issuing instructions to the firewall to drop rogue connections
C. abnormal network behavior and using it as a baseline for measuring normal activity
D. attack pattern signatures from historical data

Answer: A

Explanation:

An anomaly-based intrusion detection system (IDS) operates by gathering data on normal network behavior and using it as a baseline for measuring abnormal activity. This is important because it allows the IDS to detect any activity that is outside of the normal range of usage for the network, which can help to identify potential malicious activity or security threats. Additionally, the IDS will monitor for any changes in the baseline behavior and alert the administrator if any irregularities are detected. By contrast, signature-based IDSs operate by gathering attack pattern signatures from historical data and comparing them against incoming traffic in order to identify malicious activity.

Question: 270

A penetration test was conducted by an accredited third party. Which of the following should be the information security manager's FIRST course of action?

A. Ensure a risk assessment is performed to evaluate the findings
B. Ensure vulnerabilities found are resolved within acceptable timeframes
C. Request funding needed to resolve the top vulnerabilities
D. Report findings to senior management

Answer: D

Explanation:

Question: 271

Which of the following is the BEST course of action when an online company discovers a network attack in progress?

A. Dump all event logs to removable media
B. Isolate the affected network segment
C. Enable trace logging on ail events

D. Shut off all network access points

Answer: B

Explanation:

The BEST course of action when an online company discovers a network attack in progress is to isolate the affected network segment. This prevents the attacker from gaining further access to the network and limits the scope of the attack. Dumping event logs to removable media and enabling trace logging may be useful for forensic purposes, but should not be the first course of action in the midst of an active attack. Shutting off all network access points would be too drastic and would prevent legitimate traffic from accessing the network.

Question: 272

Relationships between critical systems are BEST understood by

A. evaluating key performance indicators (KPIs)
B. performing a business impact analysis (BIA)
C. developing a system classification scheme
D. evaluating the recovery time objectives (RTOs)

Answer: B

Explanation:

The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

Question: 273

To help ensure that an information security training program is MOST effective its contents should be

A. focused on information security policy.
B. aligned to business processes
C. based on employees' roles
D. based on recent incidents

Answer: C

Explanation:

"An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees."

Question: 274

Which of the following should be an information security manager's FIRST course of action when a newly introduced privacy regulation affects the business?

A. Consult with IT staff and assess the risk based on their recommendations
B. Update the security policy based on the regulatory requirements
C. Propose relevant controls to ensure the business complies with the regulation
D. Identify and assess the risk in the context of business objectives

Answer: D

Explanation:

Identify and assess the risk in the context of business objectives. Before making any changes to the security policy or introducing any new controls, the information security manager should first identify and assess the risk that the new privacy regulation poses to the business. This should be done in the context of the overall business objectives so that the security measures introduced are tailored to meet the specific needs of the organization.

Question: 275

Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?

A. Monitor the effectiveness of controls
B. Update the risk assessment framework
C. Review the inherent risk level
D. Review the risk probability and impact

Answer: A

Explanation:

If the residual risk of the business activity is lower than the acceptable risk level, it means that the existing controls are effectively mitigating the identified risks. In this case, the best course of action is to monitor the effectiveness of the controls and ensure they remain effective. The information security manager should review and test the controls periodically to ensure that they continue to provide adequate protection. It is also essential to update the risk assessment framework to reflect changes in the business environment or risk landscape.

Question: 276

Which of the following is the responsibility of a risk owner?

A. Implementing risk treatment plan activities with control owners
B. Evaluating control effectiveness
C. Approving risk treatment plans
D. Approving the selection of risk mitigation measures

Answer: C

Explanation:

A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk. While risk assessments, determining the organization's risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

Question: 277

Which of the following is the MOST important requirement for a successful security program?

A. Mapping security processes to baseline security standards
B. Penetration testing on key systems
C. Management decision on asset value
D. Nondisclosure agreements (NDA) with employees

Answer: C

Explanation:

"A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value."

Question: 278

A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

A. Employee training on ransomware
B. A properly tested ofline backup system

C. A continual server replication process
D. A properly configured firewall

Answer: B

Explanation:

The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested ofline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested ofline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested ofline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures. Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware. However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable. A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

Question: 279

An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?

A. Initiate incident response.
B. Disable remote
C. Initiate a device reset.
D. Conduct a risk assessment.

Answer: A

Explanation:

Initiating incident response is the first course of action for an information security manager when an employee reports the loss of a personal mobile device containing corporate information. This will help to contain the incident, assess the impact, and take appropriate measures to prevent or mitigate further damage. According to ISACA, incident management is one of the key processes for information security governance. Initiating a device reset, disabling remote access, and conducting a risk assessment are possible subsequent actions, but they should be part of the incident response plan. Reference: 1: Find, lock, or erase a lost Android device - Google Account Help 2: Find, lock, or erase a lost Android device - Android Help 3: Lost or Stolen Mobile Device Procedure - Information Security Office : CISM Practice Quiz | CISM Exam Prep | ISACA : 200 CISM Exam Prep Questions | Free Practice Test | Simplilearn : CISM practice questions to prep for the exam | TechTarget

Question: 280

When developing a business case to justify an information security investment, which of the following would BEST enable an informed decision by senior management?

A. The information security strategy
B. Losses due to security incidents
C. The results of a risk assessment
D. Security investment trends in the industry

Answer: C

Explanation:

The results of a risk assessment would best enable an informed decision by senior management when developing a business case to justify an information security investment. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the organization's assets and processes, as well as the potential impact and likelihood of occurrence. A risk assessment will also provide a basis for selecting and evaluating the effectiveness of controls to mitigate the risks. According to CISA, developing a business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment1. The information security strategy, losses due to security incidents, and security investment trends in the industry are possible inputs or outputs of a risk assessment, but they are not sufficient to enable an informed decision by senior management. Reference: 1: The Business Case for Security - CISA 2: The Business Case for Security | CISA 3: #HowTo: Build a Business Case for Cybersecurity Investment 4: Making the Business Case for Information Security

Question: 281

Which risk is introduced when using only sanitized data for the testing of applications?

A. Data loss may occur during the testing phase.
B. Data disclosure may occur during the migration event
C. Unexpected outcomes may arise in production
D. Breaches of compliance obligations will occur.

Answer: C

Explanation:

Unexpected outcomes may arise in production when using only sanitized data for the testing of applications. Sanitized data is data that has been purposely and permanently deleted or modified to prevent unauthorized access or misuse. Sanitized data may not reflect the real characteristics, patterns, or behaviors of the original data, and thus may not be suitable for testing applications that rely on data quality and accuracy. According to NIST, data sanitization methods can affect the usability of data for testing purposes1. The other options are not risks introduced by using sanitized data for testing applications, but rather risks that can be mitigated by using

sanitized data. Data loss, data disclosure, and breaches of compliance obligations are possible consequences of using unsanitized data that contains sensitive or confidential information. Reference: 2: What is Data Sanitization? | Data Erasure Methods | Imperva 3: Data sanitization techniques: Standards, practices, legislation 1: Data sanitization – Wikipedia

Question: 282

Which of the following is the BEST method to ensure compliance with password standards?

A. Implementing password-synchronization software
B. Using password-cracking software
C. Automated enforcement of password syntax rules
D. A user-awareness program

Answer: C

Explanation:

Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security. Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of

passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. Reference: 1: NIST Password Guidelines and Best Practices for 2020 - Auth0 2: Password synchronization - Wikipedia 3:

Question: 283

Which of the following factors has the GREATEST influence on the successful implementation of information security strategy goals?

A. Regulatory requirements
B. Compliance acceptance
C. Management support
D. Budgetary approval

Answer: C

Explanation:

Management support is the factor that has the greatest influence on the successful implementation of information security strategy goals. Management support refers to the commitment and involvement of senior executives and other key stakeholders in defining, approving, funding, and overseeing the information security strategy. Management support is essential for aligning the information security strategy with the business objectives, ensuring adequate resources and budget, fostering a security-aware culture, and enforcing accountability and compliance. According to ISACA, management support is one of the critical success factors for information security governance1. The other options are not factors that influence the successful implementation of information security strategy goals, but rather outcomes or components of the information security strategy. Regulatory requirements are external obligations that the information security strategy must comply with2. Compliance acceptance is the degree to which the organization adheres to the information security policies and standards3. Budgetary approval is the process of allocating financial resources for the information security activities and initiatives4. Reference: 2: Information Security: Goals, Types and Applications - Exabeam 3: How to develop a cybersecurity strategy: Step-by-step guide 4: Information Security Goals And Objectives 1: The Importance of Building an Information Security Strategic Plan

Question: 284

Management has announced the acquisition of a new company. The information security manager of the parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies. To BEST address this concern, the information security manager should:

A. review access rights as the acquisition integration occurs.
B. perform a risk assessment of the access rights.
C. escalate concerns for conflicting access rights to management.
D. implement consistent access control standards.

Answer: B

Explanation:

Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls1. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a

risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units. Reference: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M&A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M&A integration | Bain & Company : Cracking the code to successful postmerger integration

Question: 285

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance.

Which of the following would provide the MOST useful information for planning purposes? »

A. Results from a business impact analysis (BIA)
B. Deadlines and penalties for noncompliance
C. Results from a gap analysis
D. An inventory of security controls currently in place

Answer: C

Explanation:

Results from a gap analysis would provide the most useful information for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. A gap analysis is an assessment of the difference between an organization's current state of compliance and its desired level or standard. It is a process used to identify potential areas for

improvement by comparing actual performance with expected performance. A gap analysis can help to prioritize the actions needed to close the gaps and comply with the regulatory requirements, as well as to estimate the resources and time required for each action1. The other options are not as useful as results from a gap analysis for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. Deadlines and penalties for noncompliance are important factors to consider, but they do not provide information on how to achieve compliance or what actions are needed2. Results from a business impact analysis (BIA) are useful for identifying the critical processes and assets that need to be protected, but they do not provide information on how to comply with the regulatory requirements or what actions are needed3. An inventory of security controls currently in place is useful for assessing the current state of compliance, but it does not provide information on how to comply with the regulatory requirements or what actions are needed4. Reference: 3: Business impact analysis (BIA) - Wikipedia 2: Compliance Gap Analysis & Effectiveness Evaluation | SMS 1: What is Gap Analysis in Compliance | Scytale 4: Gap Analysis & Risk Assessment — Riddle Compliance

Question: 286

Which of the following documents should contain the INITIAL prioritization of recovery of services?

A. IT risk analysis
B. Threat assessment
C. Business impact analysis (BIA)

D. Business process map

Answer: C

Explanation:

A business impact analysis (BIA) is the document that should contain the initial priori-tization of recovery of services. A BIA is a process of identifying and analyzing the po-tential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:

- Identifying the critical business functions and processes that support the organization's mission and objectives.
- Estimating the maximum tolerable downtime (MTD) for each function or process, which is the longest time that the organization can afford to be without that function or process before suffering unacceptable consequences.
- Assessing the potential impacts of disruptions to each function or process, such as finan-cial losses, reputational damage, legal liabilities, regulatory penalties, customer dissatis-faction, etc.
- Prioritizing the recovery of functions or processes based on their MTDs and impacts, and assigning recovery time objectives (RTOs) and recovery point objectives (RPOs) for each function or process. RTOs are the target times for restoring functions or processes after a disruption, while RPOs are the acceptable amounts of data loss in case of a disruption.
- Identifying the resources and dependencies required for each function or process, such as staff, equipment, software, data, suppliers, customers, etc.

A BIA provides the basis for developing a business continuity plan (BCP), which is a document that outlines the strategies and procedures for ensuring the continuity or re-covery of critical business functions and processes in the event of a disruption2. The other options are not documents that

should contain the initial prioritization of recov-ery of services. An IT risk analysis is a process of identifying and evaluating the threats and vulnerabilities that affect the IT systems and assets of an organization. It helps to determine the likelihood and impact of potential IT incidents, and to select and imple-ment appropriate controls to mitigate the risks3. A threat assessment is a process of identifying and analyzing the sources and capabilities of adversaries that may pose a threat to an organization's security. It helps to determine the level of threat posed by different actors, and to develop countermeasures to prevent or respond to attacks. A business process map is a visual representation of the activities, inputs, outputs, roles, and resources involved in a business process. It helps to understand how a process works, how it can be improved, and how it relates to other processes. Reference: 1: Business impact analysis (BIA) - Wikipedia 2: Business continuity plan - Wikipedia 3: IT risk management - Wikipedia : Threat assessment - Wikipedia : Business process map-ping - Wikipedia

Question: 287

A newly appointed information security manager of a retailer with multiple stores discovers an HVAC (heating, ventilation, and air conditioning) vendor has remote access to the stores to enable realtime monitoring and equipment diagnostics. Which of the following should be the information security manager's FIRST course of action?

A. Conduct a penetration test of the vendor.
B. Review the vendor's technical security controls

C. Review the vendor contract
D. Disconnect the real-time access

Answer: C

Explanation:

Reviewing the vendor contract should be the information security manager's first course of action when discovering an HVAC vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. The vendor contract should specify the terms and conditions of the vendor's access to the retailer's network, such as the scope, purpose, duration, frequency, and method of access. The vendor contract should also define the roles and responsibilities of both parties regarding security, privacy, compliance, liability, and incident response. Reviewing the vendor contract will help the information security manager to understand the contractual obligations and expectations of both parties, and to identify any gaps or issues that need to be addressed or resolved1. The other options are not the first course of action for the information security manager when discovering an HVAC vendor has remote access to the stores. Conducting a penetration test of the vendor may be a useful way to assess the vendor's security posture and potential vulnerabilities, but it should be done with the vendor's consent and cooperation, and after reviewing the vendor contract2. Reviewing the vendor's technical security controls may be a necessary step to verify the vendor's compliance with security standards and best practices, but it should be done after reviewing the vendor contract and in accordance with the agreed-upon audit procedures3.
Disconnecting the real-time access may be a drastic measure that could disrupt the vendor's service delivery and violate the vendor contract, unless there is a clear and imminent threat or breach that warrants such action. Reference: 1: Vendor Access: Addressing the Security Challenge with Urgency -

BeyondTrust 2: Penetration Testing - NIST 3: Reduce Risk from Third Party Access | BeyondTrust : Third-Party Vendor Security Risk Management & Prevention

Question: 288

A balanced scorecard MOST effectively enables information security:

A. project management
B. governance.
C. performance.
D. risk management.

Answer: B

Explanation:

A balanced scorecard most effectively enables information security govern-ance. Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are managed effectively and efficiently1. A balanced scorecard is a tool for meas-uring and communicating the performance and progress of an organization toward its strategic goals. It typically includes

four perspectives: financial, customer, internal pro-cess, and learning and growth2. A balanced scorecard can help information security managers to:

- Align information security objectives with business objectives and communicate them to senior management and other stakeholders
- Monitor and report on the effectiveness and efficiency of information security processes and controls
- Identify and prioritize improvement opportunities and corrective actions
- Demonstrate the value and benefits of information security investments
- Foster a culture of security awareness and continuous learning

Several sources have proposed models or frameworks for applying the balanced scorecard approach to information security governance34 . The other options are not the most effective applications of a balanced scorecard for information security. Pro-ject management is the process of planning, executing, monitoring, and closing pro-jects to achieve specific objectives within constraints such as time, budget, scope, and quality. A balanced scorecard can be used to measure the performance of individual projects or project portfolios, but it is not specific to information security projects. Performance is the degree to which an organization or a process achieves its objectives or meets its standards. A balanced scorecard can be used to measure the performance of information security processes or functions, but it is not limited to performance measurement. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks that affect an organization's objec-tives. A balanced scorecard can be used to measure the risk exposure and risk appetite of an organization, but it is not a tool for risk assessment or treatment. Reference: 1: Information Security Governance - ISACA 2: Balanced scorecard - Wikipedia 3: Key Per-formance Indicators for Security Governance Part 1 - ISACA 4: A Strategy Map for Se-curity Leaders: Applying the Balanced Scorecard Framework to Information Security - Security Intelligence : How to Measure Security From a Governance Perspective - ISA-CA : Project management - Wikipedia : Performance measurement - Wikipedia : Risk management - Wikipedia

Question: 289

When creating an incident response plan, the PRIMARY benefit of establishing a clear definition of a security incident is that it helps to:

A. the incident response process to stakeholders
B. adequately staff and train incident response teams.
C. develop effective escalation and response procedures.
D. make tabletop testing more effective.

Answer: C

Explanation:

The primary benefit of establishing a clear definition of a security incident is that it helps to develop effective escalation and response procedures. A security incident is an event or an attempt that disrupts or threatens the normal operations, security, or privacy of an organization's information or systems1. A clear definition of a security in-cident helps to:

- Distinguish between normal and abnormal events, and between security-relevant and non-security-relevant events
- Determine the severity and impact of an incident, and the appropriate level of response • Assign roles and responsibilities for incident detection, reporting, analysis, containment, eradication, recovery, and post-incident activities

- Establish criteria and thresholds for escalating incidents to higher authorities or external parties
- Define the communication channels and protocols for incident notification and coordina-tion
- Document the incident response process and procedures in a formal plan

According to NIST, a clear definition of a security incident is one of the key compo-nents of an effective incident response capability2. The other options are not the prima-ry benefits of establishing a clear definition of a security incident. Communicating the incident response process to stakeholders is important, but it is not the main purpose of defining a security incident. Adequately staffing and training incident response teams is essential, but it depends on other factors besides defining a security inci-dent. Making tabletop testing more effective is a possible outcome, but not a direct benefit of defining a security incident. Reference: 2: NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide 1: NIST Glossary - Security Incident : What is a securi-ty incident? - TechTarget : 10 types of security incidents and how to handle them - TechTarget : 45 CFR § 164.304 - Definitions - Electronic Code of Federal Regulations

Question: 290

Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

A. Require remote wipe capabilities for devices.
B. Conduct security awareness training.
C. Review and update existing security policies.
D. Enforce passwords and data encryption on the devices.

Answer: C

Explanation:

The primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations is to review and update existing security policies. Security policies are the foundation of an organi-zation's security program, as they define the goals, objectives, principles, roles, respon-sibilities, and requirements for protecting information and systems. Security policies should be reviewed and updated regularly to reflect changes in the organization's envi-ronment, needs, risks, and technologies1. Implementing the use of company-owned mobile devices in its operations is a significant change that may introduce new threats and vulnerabilities, as well as new opportunities and benefits, for the organiza-tion. Therefore, the information security manager should review and update existing security policies to address the following aspects2:

- The scope, purpose, and ownership of company-owned mobile devices
- The acceptable and unacceptable use of company-owned mobile devices
- The security standards and best practices for company-owned mobile devices
- The roles and responsibilities of users, managers, IT staff, and vendors regarding compa-ny-owned mobile devices
- The procedures for provisioning, managing, monitoring, and decommissioning company-owned mobile devices
- The incident response and reporting process for company-owned mobile devices

By reviewing and updating existing security policies, the information security manager can ensure that the organization's security program is aligned with its business objec-tives and risk appetite, as well as compliant with applicable laws and regulations. The other options are not the primary responsibility of an information

security manager in an organization that is implementing the use of company-owned mobile devices in its operations. They are possible actions or controls that may be derived from or support-ed by the updated security policies. Requiring remote wipe capabilities for devices is a technical control that can help prevent data loss or theft in case of device loss or com- promise3. Conducting security awareness training is an administrative control that can help educate users about the security risks and responsibilities associated with using company-owned mobile devices. Enforcing passwords and data encryption on the de-vices is a technical control that can help protect data confidentiality and integrity on company-owned mobile devices. Reference: 1: Information Security Policy - NIST 2: Mobile Device Security Policy - SANS 3: Remote Wipe: What It Is & How It Works - Lifewire : Security Awareness Training - NIST : Mobile Device Encryption - NIST

Question: 291

An organization permits the storage and use of its critical and sensitive information on employee- owned smartphones. Which of the following is the BEST security control?

A. Establishing the authority to remote wipe
B. Developing security awareness training
C. Requiring the backup of the organization's data by the user
D. Monitoring how often the smartphone is used

Answer: A

Explanation:

The best security control for an organization that permits the storage and use of its critical and sensitive information on employee-owned smartphones is establishing the authority to remote wipe. Remote wipe is a feature that allows an authorized administrator or user to remotely erase the data on a device in case of loss, theft, or compromise1. Remote wipe can help prevent unauthorized access or disclosure of the organization's information on employee-owned smartphones, as well as protect the privacy of the employee's personal data. Remote wipe can be implemented through various methods, such as mobile device management (MDM) software, native device features, or third-party applications2. However, remote wipe requires the consent and cooperation of the employee, as well as a clear policy that defines the conditions and procedures for its use. The other options are not the best security controls for an organization that permits the storage and use of its critical and sensitive information on employee-owned smartphones. Developing security awareness training is an important measure to educate employees about the security risks and responsibilities associated with using their own smartphones for work purposes, but it does not provide a technical or physical protection for the data on the devices3. Requiring the backup of the organization's data by the user is a good practice to ensure data availability and recovery in case of device failure or loss, but it does not prevent unauthorized access or disclosure of the data on the devices4. Monitoring how often the smartphone is used is a possible way to detect abnormal or suspicious activities on the devices, but it does not prevent or mitigate the impact of a data breach on the devices. Reference: 4: Mobile Device Backup - NIST 3: Security Awareness Training - NIST 1: Remote Wipe - Lifewire 2: How Businesses with a BYOD Policy Can Secure Employee Devices - IBM : Mobile Device Security Policy – SANS

Question: 292

Labeling information according to its security classification:

A. enhances the likelihood of people handling information securely.
B. reduces the number and type of countermeasures required.
C. reduces the need to identify baseline controls for each classification.
D. affects the consequences if information is handled insecurely.

Answer: A

Explanation:

Labeling information according to its security classification enhances the likelihood of people handling information securely. Security classification is a process of categoriz-ing information based

on its level of sensitivity and importance, and applying appropri-ate security controls based on the level of risk associated with that infor-mation1. Labeling is a process of marking the information with the appropriate classifi-cation level, such as public, internal, confidential, secret, or top secret2. The purpose of labeling is to inform the users of the information about its value and protection requirements, and to guide them on how to handle it securely. Labeling can help users to:

- Identify the information they are dealing with and its classification level
- Understand their roles and responsibilities regarding the information
- Follow the security policies and procedures for the information
- Avoid unauthorized access, disclosure, modification, or destruction of the information
- Report any security incidents or breaches involving the information Labeling can also help organizations to:
- Track and monitor the information and its usage
- Enforce access controls and encryption for the information
- Audit and review the compliance with security standards and regulations for the infor-mation
- Educate and train employees and stakeholders on information security awareness and best practices

Therefore, labeling information according to its security classification enhances the likelihood of people handling information securely, as it increases their awareness and accountability, and supports the implementation of security measures. The other op-tions are not the primary benefits of labeling information according to its security clas-sification. Reducing the number and type of countermeasures required is not a benefit, but rather a consequence of applying security controls based on the classification lev-el. Reducing the need to identify baseline controls for each classification is not a bene-fit, but rather a prerequisite for labeling information according to its security classifica-tion. Affecting the consequences if information is handled insecurely is not a benefit, but rather a risk that needs to be managed by implementing appropriate security con-trols and incident response procedures. Reference: 1: Information Classification - Ad-visera 2: Information Classification in Information Security - GeeksforGeeks : Infor-mation Security Policy - NIST : Information Security Classification Framework - Queensland Government

Question: 293

Which of the following is the GREATEST benefit of information asset classification?

A. Helping to determine the recovery point objective (RPO)
B. Providing a basis for implementing a need-to-know policy
C. Supporting segregation of duties
D. Defining resource ownership

Answer: B

Explanation:

The greatest benefit of information asset classification is providing a basis for imple-menting a need- to-know policy. Information asset classification is a process of catego-rizing information based on its level of sensitivity and importance, and applying appro-priate security controls based on the level of risk associated with that information1. A need-to-know policy is a principle that states that access to information should be granted only to those individuals who require it to perform their official duties
or tasks2. The purpose of a need-to-know policy is to limit the exposure of sensitive information to unauthorized or unnecessary parties, and to reduce the risk of data breaches, leaks, or misuse. Information asset classification provides a basis for implementing a need-to-know policy by: • Defining the value and protection requirements of different types of information

- Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret
- Establishing the roles and responsibilities of information owners, custodians, and users
- Enforcing access controls and encryption for the information
- Documenting the security policies and procedures for the information

By providing a basis for implementing a need-to-know policy, information asset classi-fication can help organizations to protect their sensitive information, comply with rele-vant laws and regulations, and achieve their business objectives. The other options are not the greatest benefits of information asset classification. Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level. RPO is the acceptable amount of data loss in case of a disruption3. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a need-to-know policy. Segregation of duties is a principle that states that no single individual should have control over two or more phases of a business process or transaction that are susceptible to errors or fraud4. De-fining resource ownership is not a benefit, but rather a component of information asset classification. Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group5. Reference: 1: Information Classifi-cation - Advisera 2: Need-to-Know Principle - NIST 3: Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST : Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy - UCI

Question: 294

An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification for granting an exception to the policy?

A. The benefit is greater than the potential risk.
B. USB storage devices are enabled based on user roles.
C. Users accept the risk of noncompliance.
D. Access is restricted to read-only.

Answer: A

Explanation:

The strongest justification for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. A security policy is a document that defines the goals, objec-tives, principles, roles, responsibilities, and requirements for protecting information and systems in an organization. A security policy should be based on a risk assessment that identifies and evaluates the threats and vulnerabilities that affect the organiza-tion's assets, as well as the potential impact and likelihood of incidents. A security policy should also be aligned with the organization's business objectives and risk appe-tite1. However, there may be situations where a security policy cannot be fully enforced or complied with due to technical, operational, or business reasons. In such cases, an exception to the policy may be
requested and granted by an authorized person or body, such as a security manager or a policy committee. An exception to a security policy should be justified by a clear and compelling reason that outweighs the risk of non-compliance. An exception to a security policy should also be documented, approved, monitored, reviewed, and revoked as necessary2. The strongest justification for grant-ing an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. USB storage devices are portable devices that can store large amounts of data and can be easily connected to laptops and desktops via USB ports. They can provide several benefits for users and organizations, such as: • Enhancing data mobility and accessibility

- Improving data backup and recovery
- Supporting data sharing and collaboration
- Enabling data encryption and authentication

However, USB storage devices also pose significant security risks for users and organi-zations, such as:

- Introducing malware or viruses to laptops and desktops
- Exposing sensitive data to unauthorized access or disclosure
- Losing or stealing data due to device loss or theft
- Violating security policies or regulations

Therefore, an exception to the security policy that disables access to USB storage de-vices on laptops and desktops should only be granted if the benefit of using them is greater than the potential risk of compromising them. For example, if a user needs to transfer a large amount of data from one laptop to another in a remote location where there is no network connection available, and the data is encrypted and protected by a strong password on the USB device, then the benefit of using the USB device may be greater than the risk of losing or exposing it. The other options are not the strongest justifications for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops. Enabling USB storage devices based on user roles is not a justification, but rather a possible way of implementing a more gran-ular or flexible security policy that allows different levels of access for different types of users3. Users accepting the risk of noncompliance is not a justification, but rather a requirement for requesting an exception to a security policy that acknowledges their responsibility and accountability for any consequences of noncompliance4. Accessing being restricted to read-only is not a justification, but rather a possible control that can reduce the risk of introducing malware or viruses from USB devices to laptops and desktops5. Reference: 1: Information Security Policy - NIST 2: Policy Exception Man-agement - ISACA 3: Deploy and manage Removable Storage Access Control using In-tune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Re-movable Media Policy Writing Tips - CurrentWare

Question: 295

What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

A. Determine operational losses.
B. Improve the change control process.
C. Update the threat landscape.
D. Review the effectiveness of controls

Answer: D

Explanation:

The primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1. A business system update is a process of modifying or enhancing an information system to improve its functionality, performance, security, or compatibility. A business system update may introduce new features, fix bugs, patch vulnerabilities, or comply with new standards or regulations2. Performing a vulnerability assessment following a business system update is important because it helps to:

- Review the effectiveness of controls that are implemented to protect the information sys-tem from threats and risks
- Identify any new or residual vulnerabilities that may have been introduced or exposed by the update
- Evaluate the impact and likelihood of potential incidents that may exploit the vulnerabili-ties
- Prioritize and implement appropriate actions to address the vulnerabilities
- Verify and validate the security posture and compliance of the updated information sys-tem Therefore, the primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls that are designed to ensure the confidentiality, integrity, and availability of the information system and its data. The other options are not the primary objectives of performing a vulnerability as-sessment following a business system update. Determining operational losses is not an objective, but rather a possible consequence of not performing a vulnerability as-sessment or not addressing the identified vulnerabilities. Improving the change control process is not an objective, but rather a possible outcome of performing a vulnerability assessment and incorporating its results and recommendations into the change management cycle. Updating the threat landscape is not an objective, but rather a prereq-uisite for performing a vulnerability assessment that requires using up-to-date sources of threat intelligence and vulnerability information. Reference: 1: Vulnerability As-sessment - NIST 2: System Update - Techopedia : Vulnerability Assessment vs Penetra-tion Testing - Imperva : Change Control Process - NIST : Threat Landscape - NIST

Question: 296

Threat and vulnerability assessments are important PRIMARILY because they are:

A. used to establish security investments
B. the basis for setting control objectives.
C. elements of the organization's security posture.
D. needed to estimate risk.

Answer: D

Explanation:

Threat and vulnerability assessments are important primarily because they are the basis for setting control

objectives. Control objectives are the desired outcomes of implementing security controls, and they should be aligned with the organization's risk appetite and business objectives. Threat and vulnerability assessments help to identify the potential sources and impacts of security incidents, and to prioritize the mitigation actions based on the likelihood and severity of the risks. By conducting threat and vulnerability assessments, the organization can establish the appropriate level and type of security controls to protect its information assets and reduce the residual risk to an acceptable level. Reference = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.

Threat and vulnerability assessments are important PRIMARILY because they are the basis for setting control objectives. Control objectives are the desired outcomes or goals of implementing security controls in an information system. They are derived from the risk assessment process, which identifies and evaluates the threats and vulnerabilities that could affect the system's confidentiality, integrity and availability. By conducting threat and vulnerability assessments, an organization can determine the level of risk it faces and establish the appropriate control objectives to mitigate those risks.

Question: 297

An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?

A. Identify the skill set of the provider's incident response team.
B. Evaluate the provider's audit logging and monitoring controls.
C. Review the provider's incident definitions and notification criteria.
D. Update the incident escalation process.

Answer: C

Explanation:

When an organization is aligning its incident response capability with a public cloud service provider, the information security manager's first course of action should be to review the provider's incident definitions and notification criteria. This is because the provider's incident definitions and notification criteria may differ from the organization's own, and may affect the scope, severity, and urgency of the incidents that need to be reported and handled. By reviewing the provider's incident definitions and notification criteria, the information security manager can ensure that there is a common understanding and agreement on what constitutes an incident, how it is classified, and when and how it is communicated. This will help to avoid confusion, delays, or conflicts in the incident response process, and to establish clear roles and responsibilities between the organization and the provider. Reference = CISM Review Manual, 16th Edition, page 1021

Reviewing the provider's incident definitions and notification criteria is the FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.

Question: 298

Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?

A. Alive demonstration of the third-party supplier's security capabilities
B. The ability to i third-party supplier's IT systems and processes
C. Third-party security control self-assessment (CSA) results
D. An independent review report indicating compliance with industry standards

Answer: B

Explanation:

A service provider is a third-party supplier that provides IT services or products to an organization. A service provider should comply with the organization's information security requirements, such as policies, standards, procedures, and controls, to ensure the confidentiality, integrity, and availability of the organization's data and systems. The best way to provide an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements is to have the ability to audit the third-party supplier's IT systems and processes. An audit is a systematic and independent examination of evidence to determine the degree of conformity to predetermined criteria. An audit can verify the effectiveness and efficiency of the service provider's security controls, identify any gaps or weaknesses, and provide recommendations for improvement. An audit can also ensure that the service provider adheres to the contractual obligations and service level agreements (SLAs) with the organization. Therefore, option B is the most appropriate answer.

Option A is not the best answer because a live demonstration of the third-party supplier's security capabilities may not be comprehensive, objective, or reliable. A live demonstration may only show the positive aspects of the service provider's security, but not reveal any hidden or potential issues. A live demonstration may also be subject to manipulation or deception by the service provider.

Option C is not the best answer because third-party security control self-assessment (CSA) results may not be accurate, complete, or consistent. A self-assessment is a process where the service provider evaluates its own security controls against a set of criteria or standards. A self-assessment may be biased, subjective, or incomplete, as the service provider may not disclose or report all the relevant information or issues. A self-assessment may also vary in quality and scope depending on the service provider's expertise, resources, and methodology.

Option D is not the best answer because an independent review report indicating compliance with industry standards may not be sufficient or specific for the organization's information security requirements. An independent review is a process where an external party evaluates the service provider's security controls against a set of industry standards or best practices, such as ISO/IEC 27001, NIST CSF, PCI DSS, etc. An independent review report may provide a general overview of the

service provider's security posture, but not address the organization's unique or specific security needs, risks, or expectations. An independent review report may also be outdated, limited, or generic, as the industry standards or best practices may not reflect the current or emerging security threats or trends. Reference = CISM Review Manual 15th Edition1, pages 257-258; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 301.

An independent review report indicating compliance with industry standards BEST provides an information

security manager with sufficient assurance that a service provider complies with the organization's information security requirements. This is because an independent review report is an objective and reliable source of evidence that the service provider has implemented and maintained effective security controls that meet the industry standards and best practices. An independent review report can also provide assurance that the service provider has addressed any gaps or weaknesses identified in previous audits or assessments.

Question: 299

Which of the following should be the FIRST step in developing an information security strategy?

A. Perform a gap analysis based on the current state
B. Create a roadmap to identify security baselines and controls.
C. Identify key stakeholders to champion information security.
D. Determine acceptable levels of information security risk.

Answer: A

Explanation:

The FIRST step in developing an information security strategy is to perform a gap analysis based on the current state of the organization's information security posture. A gap analysis is a systematic process of comparing the current state with the desired state and identifying the gaps or deficiencies that need to be addressed. A gap analysis helps to establish a baseline for the information security strategy, as well as to prioritize the actions and resources needed to achieve the strategic objectives. A gap analysis also helps to align the information security strategy with the organizational goals and strategies, as well as to ensure compliance with relevant standards and regulations. Reference = CISM Review Manual, 16th Edition, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 162
first step in developing an information security strategy is to conduct a risk-aware and comprehensive inventory of your company's context, including all digital assets, employees, and vendors. Then you need to know about the threat environment and which types of attacks are a threat to your company1. This is similar to performing a gap analysis based on the current state3.

Question: 300

To help ensure that an information security training program is MOST effective, its contents should be:

A. based on recent incidents.
B. based on employees' roles.
C. aligned to business processes.
D. focused on information security policy.

Answer: B

Explanation:

To help ensure that an information security training program is MOST effective, its contents should be based

on employees' roles, as different roles have different information security responsibilities, needs, and risks. A role-based training program can tailor the content and delivery methods to suit the specific learning objectives and outcomes for each role, and enhance the relevance and retention of the information security knowledge and skills. Based on recent incidents is not the best answer, as it may not cover all the information security topics that are important for the organization, and may not address the root causes or preventive measures of the incidents. Based on employees' roles is more comprehensive and proactive than based on recent incidents. Aligned to business processes is not the best answer, as it may not reflect the individual roles and responsibilities of the employees, and may not cover all the information security aspects that are relevant for the organization. Based on employees' roles is more specific and personalized than aligned to business processes. Focused on information security policy is not the best answer, as it may not provide sufficient details or examples to help the employees understand and apply the information security policy in their daily work. Based on employees' roles is more practical and engaging than focused on information security policy. Reference = CISM Review Manual, 16th Edition, page 2241; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1002

To help ensure that an information security training program is MOST effective, its contents should be based on employees' roles. This is because different roles have different responsibilities and access levels to information and systems, and therefore face different types of threats and risks. By tailoring the training content to the specific needs and expectations of each role, the training program can increase the relevance and retention of the information security knowledge and skills for the employees. Role-based training can also help employees understand their accountability and obligations for protecting information assets in their daily tasks

Question: 301

When developing a categorization method for security incidents, the categories MUST:

A. align with industry standards.
B. be created by the incident handler.
C. have agreed-upon definitions.
D. align with reporting requirements.

Answer: C

Explanation:

When developing a categorization method for security incidents, the categories must have agreed- upon definitions. This means that the categories should be clear, consistent, and understandable for all the parties involved in the incident response process, such as the incident handlers, the stakeholders, the management, and the external authorities. Having agreed-upon definitions for the categories can help to ensure that the incidents are classified and reported accurately, that the appropriate actions and resources are allocated, and that the communication and coordination are effective. Aligning with industry standards, creating by the incident handler, and aligning with reporting requirements are not mandatory for developing a categorization method for security incidents, although they may be desirable or beneficial depending on the context and objectives of the organization. Aligning with industry standards can help to adopt best practices and benchmarks for incident response, but it may not be feasible or suitable for all types of incidents or organizations. Creating by the incident handler can allow for flexibility and customization of the categories, but it may also introduce inconsistency and ambiguity if the definitions are not shared or agreed upon by others. Aligning with reporting requirements can help to comply with legal or contractual obligations, but it may not

cover all the aspects or dimensions of the incidents that need to be categorized. Reference = CISM Review Manual, 16th Edition, pages 200-2011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 822

When developing a categorization method for security incidents, the categories MUST have agreed- upon definitions. This is because having clear and consistent definitions for each category of incidents will help to ensure a common understanding and communication among the incident response team and other stakeholders. It will also facilitate the accurate and timely identification, classification, reporting and analysis of incidents. Having agreed-upon definitions will also help to avoid confusion, ambiguity and inconsistency in the incident management process

Question: 302

Which of the following is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business?

A. Risk assessment program
B. Information security awareness training
C. Information security governance
D. Information security metrics

Answer: C

Explanation:

= Information security governance is the process of establishing and maintaining the policies, standards, frameworks, and best practices that guide the information security program of an organization. Information security governance helps to ensure that the information security program meets the needs of the business by aligning it with the organization's risk appetite, objectives, and strategy. Information security governance also helps to coordinate and integrate various assurance functions, such as risk management, compliance, audit, and incident response, to provide a holistic view of the information security posture. Information security governance is essential for achieving a

positive return on investment (ROI) from information security investments, as well as for enhancing the trust and confidence of internal and external stakeholders. Reference = CISM Review Manual (Digital Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management1. CISM Review Manual (Print Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management2. CISM ITEM DEVELOPMENT GUIDE, Domain 1: Information Security Governance, Task Statement 1.1, p. 193.

Information security governance is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business. This is because information security governance provides the strategic direction, oversight and accountability for the cybersecurity program. It also ensures that the program aligns with the business objectives, risk appetite and compliance requirements of the organization. Information security governance involves defining roles and responsibilities, establishing policies and standards, setting goals and metrics, allocating resources and monitoring performance of the cybersecurity program.

Question: 303

Which of the following provides the MOST comprehensive insight into ongoing threats facing an organization?

A. Business impact analysis (BIA)
B. Risk register
C. Penetration testing
D. Vulnerability assessment

Answer: B

Explanation:

A risk register is a document that records and tracks the information security risks facing an organization, such as their sources, impacts, likelihoods, responses, and statuses. A risk register provides the most comprehensive insight into ongoing threats facing an organization, as it covers both internal and external threats, as well as their current and potential effects on the organization's assets, processes, and objectives. A risk register also helps to prioritize and monitor the risk mitigation actions and controls, and to communicate the risk information to relevant stakeholders. Therefore, option B is the most appropriate answer.

Option A is not the best answer because a business impact analysis (BIA) is a process that identifies and evaluates the critical business functions, assets, and dependencies of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA does not provide a comprehensive insight into ongoing threats facing an organization, as it focuses more on the consequences of the threats, rather than their sources, likelihoods, or responses. A BIA is mainly used to support the business continuity and disaster recovery planning, rather than the information security risk management.

Option C is not the best answer because penetration testing is a method of simulating a malicious attack on an organization's IT systems or networks, to evaluate their security posture and identify any vulnerabilities or weaknesses that could be exploited by real attackers. Penetration testing does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers a

specific scope, target, and scenario, rather than the whole range of threats, sources, and impacts. Penetration testing is mainly used to validate and improve the technical security controls, rather than the information security risk management.

Option D is not the best answer because vulnerability assessment is a process of scanning and analyzing an organization's IT systems or networks, to detect and report any flaws or gaps that could pose a security risk. Vulnerability assessment does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers the technical aspects of the threats, rather than their business, legal, or regulatory implications. Vulnerability assessment is mainly used to identify and remediate the security weaknesses, rather than the information security risk management. Reference = CISM Review Manual 15th Edition1, pages 258-259; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 306.

A risk register provides the MOST comprehensive insight into ongoing threats facing an organization. This is because a risk register is a document that records and tracks the identified risks, their likelihood, impact, mitigation strategies, and status. A risk register helps an organization to monitor and manage the threats that could affect its objectives, assets, and operations. A risk register also helps an organization to prioritize its response efforts and allocate its resources accordingly.

Question: 304

An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?

A. Set up communication channels for the target audience.
B. Determine the needs and requirements of each audience.
C. Create a comprehensive singular communication
D. Invoke the organization's incident response plan.

Answer: D

Explanation:

The information security manager should do FIRST invoke the organization's incident response plan, which is a predefined set of procedures and guidelines for handling security incidents in a timely and effective manner. The incident response plan should include the roles and responsibilities of the incident response team, the communication protocols and channels, the escalation and reporting procedures, and the documentation and evidence collection requirements. By invoking the incident response plan, the information security manager can ensure that the incident is properly contained, analyzed, resolved, and reported, and that the appropriate stakeholders are informed and involved. The other options are not the first actions that the information security manager should take, as they are part of the communication process that follows the incident response plan. Setting up communication channels for the target audience, determining the needs and requirements of each audience, and creating a comprehensive singular communication are all important steps for communicating effectively with the board, regulatory agencies, and the media, but they are not the first priority in the event of a security incident. The information security manager should first follow the incident response plan to manage the incident and its impact, and then communicate the

relevant information to the target audience according to the plan. Reference = CISM Review Manual, 16th Edition, page 2261; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1012
Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

Question: 305

Which of the following would be MOST useful to help senior management understand the status of information security compliance?

A. Industry benchmarks
B. Key performance indicators (KPIs)
C. Business impact analysis (BIA) results
D. Risk assessment results

Answer: C

Explanation:

Key performance indicators (KPIs) are measurable values that demonstrate how effectively an organization is achieving its key objectives and goals. KPIs can help senior management understand the status of information security compliance by providing quantifiable and relevant data on the performance and progress of the information security program and processes. KPIs can also help senior management to evaluate the effectiveness and efficiency of the information security controls and activities, identify strengths and weaknesses, and make informed decisions and adjustments. KPIs should be aligned with the organization's strategy, vision, and mission, and should be SMART (specific, measurable, achievable, relevant, and time-bound). Some examples of information security KPIs are: percentage of compliance with policies and standards, number of security incidents and breaches, mean time to detect and respond to incidents, percentage of systems and applications patched, number of security awareness trainings completed, etc.

Industry benchmarks, business impact analysis (BIA) results, and risk assessment results are not the most useful to help senior management understand the status of information security compliance, although they may provide some useful information or insights. Industry benchmarks are comparative measures of the performance or practices of other organizations in the same industry or sector. Industry benchmarks can help senior management to compare and contrast their own information security performance or practices with those of their peers or competitors, and identify gaps or opportunities for improvement. However, industry benchmarks may not reflect the specific goals, needs, or context of the organization, and may not be readily available or reliable. Business impact analysis (BIA) results are the outcomes of the process of analyzing the potential impacts of disruptive events on the organization's critical business functions and processes. BIA results can help senior management to understand the dependencies, priorities, and recovery objectives of the

organization's business functions and processes, and to plan for business continuity and disaster recovery. However, BIA results do not directly measure or indicate the status of information security compliance, and may not be updated or accurate. Risk assessment results are the outcomes of the process of identifying, analyzing, and evaluating the information security risks that the organization faces. Risk assessment results can help senior management to understand the sources, causes, and consequences of information security risks, and to determine the appropriate risk responses and controls. However, risk assessment results do not directly measure or indicate the status of information security compliance, and may vary depending on the risk assessment methodology, criteria, and frequency. Reference = CISM Review Manual, 16th Edition, pages 47-481, 54-551, 69701, 72-731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 832

Key performance indicators (KPIs) are metrics that measure the effectiveness and ef-ficiency of information security processes and activities. They help senior manage-ment understand the status of information security compliance by providing relevant, timely and accurate information on the performance of security controls, the level of risk exposure, the return on security investment and the progress toward security ob-jectives. KPIs can also be used to benchmark the organization's security performance against industry standards or best practices. KPIs should be aligned with the organiza-tion's strategic goals and risk appetite, and should be reported regularly to senior management and other stakeholders.

Reference:

- 1 Key Performance Indicators for Security Governance, Part 1 - ISACA
- 2 Key Performance Indicators for Security Governance, Part 2 - ISACA
- 3 Compliance Metrics and KPIs For Measuring Compliance Effectiveness - Reciprocity
- 4 14 Cybersecurity Metrics + KPIs You Must Track in 2023 - UpGuard

Question: 306

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

A. service level agreements (SLAs)
B. security requirements for the process being outsourced.
C. risk-reporting methodologies.
D. security metrics

Answer: B

Explanation:

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus primarily on defining security requirements for the process being outsourced. Security requirements are the specifications of what needs to be done to protect the information assets from unauthorized access, use, disclosure, modification, or destruction. Security requirements should be aligned with the organization's risk appetite and

business objectives, and should cover both technical and organizational aspects of the service delivery. Security requirements should also be clear, concise, measurable, achievable, realistic, and testable. Reference = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.

Security requirements for the process being outsourced are the specifications and standards that the third party must comply with to ensure the confidentiality, integrity and availability of the critical business information. They define the roles and responsi-bilities of both parties, the security controls and measures to be implemented, the se-curity objectives and expectations, the security risks and mitigation strategies, and the security monitoring and reporting mechanisms. Security requirements are essential to protect the information assets of the organization and to establish a clear and enforceable contractual relationship with the third party.

Reference:

- 1 Outsourcing Strategies for Information Security: Correlated Losses and Security Exter-nalities - SpringerLink
- 2 What requirements must outsourcing services comply with for the European market? - CBI
- 3 Outsourcing cybersecurity: What services to outsource, what to keep in house - Infosec Institute
- 4 BCFSA outsourcing and information security guidelines - BLG

Question: 307

Which of the following BEST facilitates the effective execution of an incident response plan?

A. The plan is based on risk assessment results.
B. The response team is trained on the plan
C. The plan is based on industry best practice.
D. The incident response plan aligns with the IT disaster recovery plan (DRP).

Answer: B

Explanation:

The effective execution of an incident response plan depends largely on the competence and readiness of the response team, who are responsible for carrying out the tasks and activities defined in the plan. Therefore, the best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan, and that they are familiar with their roles, responsibilities, procedures, and tools. Training the response team on the plan will also help to improve their confidence, communication, coordination, and collaboration during an incident response. The other options are not the best ways to facilitate the effective execution of an incident response plan, although they may be important factors for developing or improving the plan. The plan should be based on risk assessment results and industry best practice, but these do not guarantee that the plan will be executed effectively. The incident response plan should align with the IT disaster recovery plan, but this does not ensure that the response team is prepared and capable of executing the plan. Reference = CISM Review Manual, 16th Edition, page 1031

The best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan. An incident response plan is a set of instructions that defines the roles, responsibilities, procedures, and tools for detecting, responding to, and recovering from security incidents. An incident response team is a group of individuals that are assigned to perform specific tasks and activities during an incident response process. The response team may include security analysts, IT staff, legal counsel, public relations, and other stakeholders. To execute an incident response plan effectively, the response team needs to be trained on the plan, which means they need to be familiar with the following aspects of the plan: The scope and objectives of the plan The roles and responsibilities of each team member The communication and escalation protocols The incident classification and prioritization criteria The incident response procedures and tools The incident documentation and reporting requirements The incident review and improvement processes By training the response team on the plan, the organization can ensure that the team members are prepared and confident to handle any security incidents that may occur, and that they can perform their tasks efficiently and consistently. The other options are not the best way to facilitate the effective execution of an incident response plan, although they may be some steps or outcomes of the process. The plan being based on risk assessment results is a desirable practice, as it ensures that the plan is aligned with the organization's risk profile and addresses the most relevant and likely threats and vulnerabilities. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The plan being based on industry best practice is a desirable practice, as it ensures that the plan follows established standards and guidelines for incident response. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The incident response plan aligning with the IT disaster recovery plan (DRP) is a desirable practice, as it ensures that the plans are consistent and coordinated in terms of objectives, scope, roles, procedures, and tools. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan

Question: 308

Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?

A. Availability of resources
B. Root cause analysis results
C. Adverse effects on the business
D. Legal and regulatory requirements

Answer: C

Explanation:

The severity hierarchy for information security incident classification should be based on the potential or actual impact of the incident on the business objectives, operations, reputation, and stakeholders. The adverse effects on the business can be measured by criteria such as financial loss, operational disruption, legal liability, regulatory compliance, customer satisfaction, and public confidence. The other options are not the primary basis for a severity hierarchy, although they may be considered as secondary factors or consequences of an incident

Question: 309

The MOST important element in achieving executive commitment to an information security governance program is:

A. a defined security framework.
B. a process improvement model
C. established security strategies.
D. identified business drivers.

Answer: D

Explanation:

The most important element in achieving executive commitment to an information security governance program is to align the program with the identified business drivers of the organization. Business drivers are the factors that influence the strategic objectives, goals, and priorities of the organization. They reflect the needs and expectations of the stakeholders, customers, regulators, and other parties that are relevant to the organization's mission and vision. By aligning the information security governance program with the business drivers, the executive can demonstrate the value and benefits of information security to the organization's performance, reputation, and competitiveness. The other options are not the most important element, although they may be part of an information security governance program. A defined security framework is a set of standards, guidelines, and best practices that provide a structure and direction for implementing information security. A process improvement model is a methodology that helps to identify, analyze, and improve the processes related to information security. Established security strategies are the plans and actions that define how information security supports and enables the business objectives and goals. These elements are important for developing and executing an information security governance program, but they do not necessarily ensure executive commitment unless they are aligned with the business drivers

Question: 310

An organization plans to leverage popular social network platforms to promote its products and services. Which of the following is the BEST course of action for the information security manager to support this initiative?

A. Establish processes to publish content on social networks.
B. Assess the security risk associated with the use of social networks.
C. Conduct vulnerability assessments on social network platforms.
D. Develop security controls for the use of social networks.

Answer: B

Explanation:

The best course of action for the information security manager to support the initiative of leveraging popular social network platforms to promote the organization's products and services is to assess the security risk associated with the use of social networks. Security risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a security risk assessment, the information security manager can provide valuable input to the decision-making process regarding the benefits and costs of using social networks, as well as the appropriate security controls and mitigation strategies to reduce the risk to an acceptable level. The other options are not the best course of action, although they may be part of the security risk management process. Establishing processes to publish content on social networks is an operational task that should be performed after assessing the security risk and implementing the necessary controls. Conducting vulnerability assessments on social network platforms is a technical activity that may not be feasible or effective, as the organization does not have control over the platforms' infrastructure and configuration. Developing security controls for the use of social networks is a preventive measure that should be based on the results of the security risk assessment and aligned with the organization's risk appetite and tolerance

Question: 311

A risk owner has accepted a large amount of risk due to the high cost of controls. Which of the following should be the information security manager's PRIMARY focus in this situation?

A. Establishing a strong ongoing risk monitoring process
B. Presenting the risk profile for approval by the risk owner
C. Conducting an independent review of risk responses
D. Updating the information security standards to include the accepted risk

Answer: A

Explanation:

The information security manager's PRIMARY focus in this situation should be establishing a strong ongoing risk

monitoring process, which is the process of tracking and evaluating the changes in the risk environment, the effectiveness of the risk responses, and the impact of the residual risk on the organization. A strong ongoing risk monitoring process can help the information security manager to identify any deviations from the expected risk level, to report any significant changes or issues to the risk owner and other stakeholders, and to recommend any adjustments or improvements to the risk management strategy. Presenting the risk profile for approval by the risk owner is not the primary focus in this situation, as it is a step that should be done before the risk owner accepts the risk, not after. Conducting an independent review of risk responses is not the primary focus in this situation, as it is a quality assurance activity that can be performed by an external auditor or a third-party expert, not by the information security manager. Updating the information security standards to include the accepted risk is not the primary focus in this situation, as it is a documentation activity that does not address the ongoing monitoring and reporting of the risk. Reference = CISM Review Manual, 16th Edition, page 2281; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1022

Question: 312

Which is following should be an information security manager's PRIMARY focus during the development of a critical system storing highly confidential data?

A. Reducing the number of vulnerabilities detected
B. Ensuring the amount of residual risk is acceptable
C. Avoiding identified system threats
D. Complying with regulatory requirements

Answer: B

Explanation:

The information security manager's primary focus during the development of a critical system storing highly confidential data should be ensuring the amount of residual risk is acceptable. Residual risk is the level of cyber risk remaining after all the security controls are accounted for, any threats have been addressed and the organization is meeting security standards. It's the risk that slips through the cracks of the system. For a critical system storing highly confidential data, the residual risk should be as low as possible, and within the organization's risk appetite and tolerance. The information security manager should monitor and review the residual risk throughout the system development life cycle, and ensure that it is communicated and approved by the appropriate stakeholders. The other options are not the primary focus, although they may be part of the security objectives and activities. Reducing the number of vulnerabilities detected is a desirable outcome, but it does not necessarily mean that the residual risk is acceptable, as some vulnerabilities may have a higher impact or likelihood than others. Avoiding identified system threats is a preventive measure, but it does not account for unknown or emerging threats that may pose a residual risk to the system. Complying with regulatory requirements is a mandatory obligation, but it does not guarantee that the residual risk is acceptable, as regulations may not cover all aspects of security or reflect the specific context and needs of the organization.

Question: 313

An organization has identified an increased threat of external brute force attacks in its environment. Which of

the following is the MOST effective way to mitigate this risk to the organization's critical systems?

A. Implement multi-factor authentication.
B. Increase the frequency of log monitoring and analysis.
C. Implement a security information and event management system (SIEM),
D. Increase the sensitivity of intrusion detection systems (IDSs).

Answer: A

Explanation:

A brute force attack is a type of cyberattack that attempts to gain unauthorized access to an account, file, or other protected information by trying different combinations of usernames and passwords until finding the correct one. Brute force attacks can be very effective if the target system has weak or default passwords, or if the attacker has access to a large number of potential credentials. To mitigate this risk, an organization should implement multi-factor authentication (MFA) for its critical systems. MFA is a security method that requires users to provide more than one piece of evidence to verify their identity before accessing a system or service. For example, MFA can involve using a password in addition to a code sent to a phone or email, or using a biometric factor such as a fingerprint or face scan. MFA can significantly reduce the impact of brute force attacks by making it harder for attackers to guess or obtain valid credentials, and by increasing the time and effort required for them to compromise the system. Reference = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.

Question: 314

The PRIMARY advantage of performing black-box control tests as opposed to white-box control tests is that they:

A. cause fewer potential production issues.
B. require less IT staff preparation.
C. simulate real-world attacks.
D. identify more threats.

Answer: C

Explanation:

The primary advantage of performing black-box control tests as opposed to white-box control tests is that they simulate real-world attacks. Black-box control tests are a software testing methodology in which the tester analyzes the functionality of an application without a thorough knowledge of its internal design. Conversely, in white-box control tests, the tester is knowledgeable of the internal design of the application and analyzes it during testing. By performing black-box control tests, the tester can mimic the perspective and behavior of an external attacker who does not have access to the source code or the implementation details of the

application. This way, the tester can evaluate how the application responds to different inputs and scenarios, and identify any vulnerabilities or errors that may affect its functionality or security. The other options are not the primary advantage of performing black-box control tests, although they may be some benefits or drawbacks depending on the context. Causing fewer potential production issues is not necessarily true, as black-box control tests may still introduce errors or disruptions to the application if not performed carefully. Requiring less IT staff preparation is not always true, as black-box control tests may still require a lot of planning and documentation to ensure adequate test coverage and quality. Identifying more threats is not necessarily true, as black-box control tests may miss some threats that are hidden in the internal logic or structure of the application.

Question: 315

Which of the following is the BEST justification for making a revision to a password policy?

A. Vendor recommendation
B. Audit recommendation
C. A risk assessment
D. Industry best practice

Answer: C

Explanation:

The best justification for making a revision to a password policy is a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a risk assessment, the organization can determine the appropriate level of security controls and measures to protect its information assets and systems, including password policies. A risk assessment can also help identify any gaps or weaknesses in the existing password policy, and provide recommendations for improvement based on the organization's risk appetite and tolerance. The other options are not the best justification for making a revision to a password policy, although they may be some inputs or outputs of the risk assessment process. A vendor recommendation is an external source of advice or guidance that may or may not be relevant or applicable to the organization's specific context and needs. A vendor recommendation should not be followed blindly without conducting a risk assessment to evaluate its suitability and effectiveness. An audit recommendation is an internal source of feedback or suggestion that may or may not be accurate or complete. An audit recommendation should not be implemented without conducting a risk assessment to verify its validity and feasibility. An industry best practice is a general standard or guideline that may or may not reflect the organization's unique characteristics and requirements. An industry best practice should not be adopted without conducting a risk assessment to customize it according to the organization's goals and priorities

Question: 316

Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?

A. Conducting periodic vulnerability assessments

B. Communicating business impact analysis (BIA) results
C. Establishing effective stakeholder relationships
D. Defining the organization's risk management framework

Answer: A

Explanation:

The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

Question: 317

Which of the following is BEST to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?

A. Projected Increase in maturity level
B. Estimated reduction in risk
C. Projected costs over time
D. Estimated increase in efficiency

Answer: B

Explanation:

The best thing to include in a business case when the return on investment (ROI) for an information security

initiative is difficult to calculate is an estimated reduction in risk. Risk reduction is the expected benefit of implementing an information security initiative, as it reduces the likelihood and impact of threats and vulnerabilities that may affect the organization's information assets and systems. By estimating the reduction in risk, the information security manager can demonstrate the

value and benefits of the information security initiative to the organization's performance, reputation, and competitiveness. The information security manager can also compare the estimated reduction in risk with the estimated cost of the information security initiative to determine its costeffectiveness and feasibility. The other options are not the best thing to include in a business case, although they may be some inputs or outputs of the risk assessment process. A projected increase in maturity level is a potential outcome of implementing an information security initiative, as it improves the organization's capabilities and processes for managing information security risks. However, it does not necessarily reflect the actual reduction in risk or the ROI of the information security initiative. A projected cost over time is a component of calculating the ROI of an information security initiative, as it reflects the total cost of ownership and maintenance of the initiative. However, it does not indicate the expected benefit or value of the initiative. An estimated increase in efficiency is a possible benefit of implementing an information security initiative, as it may enhance the organization's productivity and performance. However, it may not be directly related to the reduction in risk or the ROI of the information security initiative.

Question: 318

Which of the following is the MOST important issue in a penetration test?

A. Having an independent group perform the test
B. Obtaining permission from audit
C. Performing the test without the benefit of any insider knowledge
D. Having a defined goal as well as success and failure criteria

Answer: D

Explanation:

The most important issue in a penetration test is having a defined goal as well as success and failure criteria. A penetration test is a simulated cyber attack against a computer system or an application to check for exploitable vulnerabilities. The goal of a penetration test is to identify and evaluate the security risks and weaknesses of the target system or application, and to provide recommendations for improvement. The success and failure criteria of a penetration test are the metrics and indicators that measure the effectiveness and efficiency of the test, and the extent to which the test achieves its goal. By having a defined goal as well as success and failure criteria, the penetration tester can plan and execute the test in a systematic and structured manner, and can communicate and report the results and findings in a clear and concise way. The other options are not the most important issue in a penetration test, although they may be some factors or considerations that affect the test. Having an independent group perform the test is a desirable practice, as it can provide an unbiased and objective assessment of the target system or application. However, it is not essential, as long as the penetration tester follows ethical hacking principles and standards. Obtaining permission from audit is a mandatory requirement, as it ensures that the penetration test is authorized and compliant with the organization's policies and regulations. However, it is not an issue, as it is a prerequisite for conducting the test. Performing the test without the benefit of any insider knowledge is an optional approach,

as it simulates a real-world attack by an external hacker who does not have access to the internal design or configuration of the target system or application. However, it is not always feasible

or effective, as some vulnerabilities may be hidden or inaccessible from an outsider's perspective.

Question: 319

Which of the following is the MOST important consideration when determining which type of failover site to employ?

A. Reciprocal agreements
B. Disaster recovery test results
C. Recovery time objectives (RTOs)
D. Data retention requirements

Answer: C

Explanation:

The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources. Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

Question: 320

What should be an information security manager's FIRST step when developing a business case for a new intrusion detection system (IDS) solution?

A. Define the issues to be addressed.
B. Perform a cost-benefit analysis.
C. Calculate the total cost of ownership (TCO).
D. Conduct a feasibility study.

Answer: A

Explanation:

The first step when developing a business case for a new intrusion detection system (IDS) solution is to define the issues to be addressed. A business case is a document that provides the rationale and justification for initiating a project or investment. It typically includes information such as the problem statement, the objectives, the alternatives, the costs and benefits, the risks and assumptions, and the expected outcomes. The first step in developing a business case is to define the issues to be addressed, which means identifying and describing the current situation, the problems or challenges faced by the organization, and the needs or opportunities for improvement. By defining the issues to be addressed, the information security manager can establish the scope and purpose of the business case, and provide a clear and compelling problem statement that explains why a new IDS solution is needed. The other options are not the first step when developing a business case for a new IDS solution, although they may be part of the subsequent steps. Performing a cost-benefit analysis is a step that involves comparing the costs and benefits of different alternatives, including the new IDS solution and the status quo. A cost-benefit analysis can help evaluate and justify the feasibility and desirability of each alternative, and support the decisionmaking process. Calculating the total cost of ownership (TCO) is a step that involves estimating the direct and indirect costs associated with acquiring, operating, maintaining, and disposing of an asset or a system over its entire life cycle. A TCO calculation can help determine the long-term financial implications of investing in a new IDS solution, and compare it with other alternatives. Conducting a feasibility study is a step that involves assessing the technical, operational, legal, and economic aspects of implementing a project or an investment. A feasibility study can help identify and mitigate any potential issues or risks that may affect the success of the project or investment, and provide recommendations for improvement

Question: 321

Of the following, who is MOST appropriate to own the risk associated with the failure of a privileged access control?

A. Data owner
B. Business owner
C. Information security manager
D. Compliance manager

Answer: B

Explanation:

The business owner is the most appropriate person to own the risk associated with the failure of a privileged access control because they are ultimately responsible for the protection and use of the information in their

business unit1. The data owner is responsible for determining the access rights for specific data sets, but not for the access control mechanisms2. The information security manager is responsible for implementing and enforcing the security policies and standards, but not for owning the risk3. The compliance manager is responsible for ensuring that the organization meets the regulatory requirements, but not for owning the risk3.

Reference: 1 https://www.cyberark.com/resources/blog/how-do-you-prioritize-risk-for-privileged- access-management 3 https://www.isaca.org/resources/isaca-journal/issues/2017/volume- 1/capability-framework-for-privileged-access-management 2 https://security.stackexchange.com/questions/218049/what-is-the-difference- between-data-owner-data-custodian-and-system-owner

Question: 322

Which of the following roles is MOST appropriate to determine access rights for specific users of an application?

A. Data owner
B. Data custodian
C. System administrator
D. Senior management

Answer: A

Explanation:

The data owner is the most appropriate role to determine access rights for specific users of an application because they have legal rights and complete control over data elements4. They are also responsible for approving data glossaries and definitions, ensuring the accuracy of information, and supervising operations related to data quality5. The data custodian is responsible for the safe custody, transport, and storage of the data and implementation of business rules, but not for determining access rights4. The system administrator is responsible for managing the security and storage infrastructure of data sets according to the organization's data governance policies, but not for determining access rights5. Senior management is responsible for setting the strategic direction and priorities for data governance, but not for determining access rights5.

Reference: 5 https://www.cpomagazine.com/cyber-security/data-owners-vs-data-stewards-vs-data-custodians-the-3-types-of-data-masters-and-why-you-should-employ-them/ 4 https://cloudgal42.com/data-privacy-difference-between-data-owner-controller-and-data-custodian-processor/

Question: 323

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized disclosure?

A. Integrity
B. Authenticity
C. Confidentiality

D. Nonrepudiation

Answer: C

Explanation:

Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial.

Reference: https://www.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

Question: 324

Which of the following provides the BEST evidence that a recently established infofmation security program is effective?

A. The number of reported incidents has increased
B. Regular IT balanced scorecards are communicated.
C. Senior management has reported fewer junk emails.
D. The number of tickets associated with IT incidents have stayed consistent

Answer: A

Explanation:

The number of reported incidents has increased is the best evidence that a recently established information security program is effective because it indicates that the organization has improved its detection and reporting capabilities and has raised awareness among employees about security issues. Regular IT balanced scorecards are communicated is not a good evidence because it does not measure the actual performance or outcomes of the security program. Senior management has reported fewer junk emails is not a good evidence because it does not reflect the overall security posture or maturity of the organization. The number of tickets associated with IT incidents have stayed consistent is not a good evidence because it does not show any improvement or reduction in security incidents or risks. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004 https://www.isaca.org/resources/isaca-journal/issues/2014/volume-6/how-to-measure-the-effectiveness-of-your-information-security-management-system

Question: 325

Recovery time objectives (RTOs) are an output of which of the following?

A. Business continuity plan (BCP)
B. Disaster recovery plan (DRP)
C. Service level agreement (SLA)
D. Business impact analysis (BIA)

Answer: D

Explanation:

Business impact analysis (BIA) is the process that provides the output of recovery time objectives (RTOs), which are the maximum acceptable time frames for restoring business functions or processes after a disruption. Business continuity plan (BCP) is the document that describes the strategies and procedures for ensuring the continuity of critical business functions or processes in the event of a disruption. Disaster recovery plan (DRP) is the document that describes the technical steps and resources for restoring IT systems and data in the event of a disruption. Service level agreement (SLA) is the document that defines the expectations and obligations between a service provider and a service consumer, such as availability, performance, and security. Reference: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/business-impact-analysis-bia- and-disaster-recovery-planning-drp https://www.isaca.org/resources/isaca- journal/issues/2017/volume-6/service-level-agreements-in-the-cloud

Question: 326

Which of the following would MOST effectively ensure that a new server is appropriately secured?

A. Performing secure code reviews
B. Enforcing technical security standards
C. Conducting penetration testing
D. Initiating security scanning

Answer: B

Explanation:

Enforcing technical security standards is the most effective way to ensure that a new server is appropriately secured because it ensures that the server complies with the organization's security policies and best practices, such as encryption, authentication, patching, and hardening. Performing secure code reviews is not relevant for securing a new server, unless it is running custom applications

that need to be verified for security flaws. Conducting penetration testing is not sufficient for securing a new server, because it only identifies vulnerabilities that can be exploited by attackers, but does not fix them. Initiating security scanning is not sufficient for securing a new server, because it only detects known vulnerabilities or misconfigurations, but does not enforce security standards or remediate issues. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume- 4/technical-security-standards-for-information-systems https://www.isaca.org/resources/isaca- journal/issues/2017/volume-3/secure-code-review https://www.isaca.org/resources/isaca- journal/issues/2017/volume-2/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

Question: 327

Which of the following metrics provides the BEST evidence of alignment of information security governance with corporate governance?

A. Average return on investment (ROI) associated with security initiatives
B. Average number of security incidents across business units
C. Mean time to resolution (MTTR) for enterprise-wide security incidents
D. Number of vulnerabilities identified for high-risk information assets

Answer: A

Explanation:

Average return on investment (ROI) associated with security initiatives is the best metric to provide evidence of alignment of information security governance with corporate governance because it demonstrates the value and benefits of security investments to the organization's strategic goals and objectives. Average number of security incidents across business units is not a good metric because it does not measure the effectiveness or efficiency of security initiatives or their alignment with corporate governance. Mean time to resolution (MTTR) for enterprise-wide security incidents is not a good metric because it does not measure the impact or outcome of security initiatives or their alignment with corporate governance. Number of vulnerabilities identified for high-risk information assets is not a good metric because it does not measure the performance or improvement of security initiatives or their alignment with corporate governance. Reference: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of- information-security-investments https://www.isaca.org/resources/isaca- journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-information-security- governance

Question: 328

A daily monitoring report reveals that an IT employee made a change to a firewall rule outside of the change control process. The information security manager's FIRST step in addressing the issue should be to:

A. require that the change be reversed
B. review the change management process
C. perform an analysis of the change
D. report the event to senior management

Answer: C

Explanation:

Performing an analysis of the change is the first step in addressing the issue of an IT employee making a change to a firewall rule outside of the change control process because it helps to understand the reason, impact, and risk of the change and to decide whether to approve, reject, or reverse it. Requiring that the change be reversed is not the first step because it may cause more disruption or damage without

proper analysis and testing. Reviewing the change management process is not the first step because it does not address the specific issue or incident at hand, but rather focuses on improving the process for future changes. Reporting the event to senior management is not the first step because it does not resolve the issue or incident, but rather escalates it without sufficient information or recommendation. Reference: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/change-management-in-the- age-of-digital-transformation https://www.isaca.org/resources/isaca-journal/issues/

Question: 329

Which of the following BEST enables an organization to enhance its incident response plan processes and procedures?

A. Security risk assessments
B. Lessons learned analysis
C. Information security audits
D. Key performance indicators (KPIs)

Answer: B

Explanation:

Lessons learned analysis is the best way to enable an organization to enhance its incident response plan processes and procedures because it helps to identify the strengths and weaknesses of the current plan, capture the feedback and recommendations from the incident responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Security risk assessments are not directly related to enhancing the incident response plan, but rather to identifying and evaluating the security risks and controls of the organization. Information security audits are not directly related to enhancing the incident response plan, but rather to verifying and validating the compliance and effectiveness of the security policies and standards of the organization. Key performance indicators (KPIs) are not directly related to enhancing the incident response plan, but rather to measuring and reporting the performance and progress of the security objectives and initiatives of the organization. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons- learned https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/security-risk- assessment-for-a-cloud-based-enterprise-resource-planning-system https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the- effectiveness-of-information-security-using-iso-27004 https://www.isaca.org/resources/isaca- journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security- management-system

Question: 330

For the information security manager, integrating the various assurance functions of an organization is important PRIMARILY to enable:

A. consistent security.
B. comprehensive audits
C. a security-aware culture

D. compliance with policy

Answer: A

Explanation:

Consistent security is the primary reason for integrating the various assurance functions of an organization for the information security manager because it ensures that the security policies and standards are applied uniformly and effectively across different domains, processes, and systems of the organization. Comprehensive audits are not the primary reason for integrating the various assurance functions, but rather a possible outcome or benefit of doing so. A security-aware culture is not the primary reason for integrating the various assurance functions, but rather a desirable state or goal of the organization. Compliance with policy is not the primary reason for integrating the various assurance functions, but rather a basic requirement or expectation of the organization. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance- functions https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure- the-effectiveness-of-your-information-security-management-system

Question: 331

Which of the following BEST facilitates effective strategic alignment of security initiatives?

A. The business strategy is periodically updated
B. Procedures and standards are approved by department heads.
C. Periodic security audits are conducted by a third-party.
D. Organizational units contribute to and agree on priorities

Answer: D

Explanation:

Organizational units contribute to and agree on priorities is the best way to facilitate effective strategic alignment of security initiatives because it ensures that the security initiatives are aligned with the business goals and objectives, supported by relevant stakeholders, and prioritized based on risk and value. The business strategy is periodically updated is not sufficient to facilitate effective strategic alignment of security initiatives because it does not involve collaboration or communication between different organizational units. Procedures and standards are approved by department heads is not sufficient to facilitate effective strategic alignment of security initiatives because it does not reflect the strategic direction or vision of the organization. Periodic security audits are conducted by a third-party is not sufficient to facilitate effective strategic alignment of security initiatives because it does not address the planning or implementation of security initiatives. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-information-security- governance

Question: 332

Which of the following is MOST important for the effective implementation of an information security

governance program?

A. Employees receive customized information security training
B. The program budget is approved and monitored by senior management
C. The program goals are communicated and understood by the organization.
D. Information security roles and responsibilities are documented.

Answer: C

Explanation:

The program goals are communicated and understood by the organization is the most important factor for the effective implementation of an information security governance program because it ensures that the program is aligned with the business objectives and supported by the stakeholders. Employees receive customized information security training is not the most important factor, but rather a means to achieve the program goals and raise awareness among the staff. The program budget is approved and monitored by senior management is not the most important factor, but rather a resource to enable the program activities and measure its performance. Information security roles and responsibilities are documented is not the most important factor, but rather a way to define and assign the program tasks and accountabilities. Reference: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the- effectiveness-of-information-security-governance https://www.isaca.org/resources/isaca- journal/issues/2016/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives

Question: 333

Of the following, who is accountable for data loss in the event of an information security incident at a third-party provider?

A. The information security manager
B. The service provider that hosts the data
C. The incident response team
D. The business data owner

Answer: D

Explanation:

The business data owner is accountable for data loss in the event of an information security incident at a third-party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third-party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2018/volume- 3/incident-

response-lessons-learned

Question: 334

Senior management has expressed concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations Which of the following BEST indicates that the information security manager has tuned the system to address this concern?

A. Increasing false negatives
B. Decreasing false negatives
C. Decreasing false positives
D. Increasing false positives

Answer: C

Explanation:

Decreasing false positives is the best indicator that the information security manager has tuned the system to address senior management's concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations. False positives are alerts generated by the IPS when it mistakenly blocks legitimate traffic or activity, causing disruption or downtime. Decreasing

false positives means that the IPS has been configured to reduce such errors and minimize unnecessary interruptions. Increasing false negatives is not a good indicator because it means that the IPS has failed to detect or block malicious traffic or activity, increasing the risk of compromise or damage. Decreasing false negatives is not a good indicator because it does not affect business operations, but rather improves security detection or prevention. Increasing false positives is not a good indicator because it means that the IPS has increased its errors and interruptions, worsening senior management's concern. Reference: https://www.isaca.org/resources/isaca- journal/issues/2017/volume-6/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

Question: 335

Which of the following BEST describes a buffer overflow?

A. A function is carried out with more data than the function can handle
B. A program contains a hidden and unintended function that presents a security risk
C. Malicious code designed to interfere with normal operations
D. A type of covert channel that captures data

Answer: A

Explanation:

A buffer overflow is a software coding error or vulnerability that occurs when a function is carried out with

more data than the function can handle, resulting in adjacent memory locations being overwritten or corrupted by the excess data1. A program contains a hidden and unintended function that presents a security risk is not a buffer overflow, but rather a backdoor2. Malicious code designed to interfere with normal operations is not a buffer overflow, but rather malware3. A type of covert channel that captures data is not a buffer overflow, but rather a keylogger.
Reference: 1 https://www.fortinet.com/resources/cyberglossary/buffer-overflow 2 https://www.fortinet.com/resources/cyberglossary/backdoor 3 https://www.fortinet.com/resources/cyberglossary/malware https://www.fortinet.com/resources/cyberglossary/keylogger

Question: 336

Which of the following is the BEST method for determining whether a firewall has been configured to provide a comprehensive perimeter defense9

A. A validation of the current firewall rule set
B. A port scan of the firewall from an internal source
C. A ping test from an external source
D. A simulated denial of service (DoS) attack against the firewall

Answer: A

Explanation:

A validation of the current firewall rule set is the best method for determining whether a firewall has been configured to provide a comprehensive perimeter defense because it verifies that the firewall rules are consistent, accurate, and effective in allowing or blocking traffic according to the security policies and standards of the organization. A port scan of the firewall from an internal source is not a good method because it does not test the firewall's behavior from an external perspective, which is more relevant for perimeter defense. A ping test from an external source is not a good method because it only tests the firewall's availability and responsiveness, not its security or functionality. A simulated denial of service (DoS) attack against the firewall is not a good method because it only tests the firewall's resilience and performance under high traffic load, not its security or functionality. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security- standards-for-information-systems https://www.isaca.org/resources/isaca- journal/issues/2017/volume-2/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

Question: 337

Which of the following BEST enables an organization to maintain legally admissible evidence7

A. Documented processes around forensic records retention
B. Robust legal framework with notes of legal actions
C. Chain of custody forms with points of contact
D. Forensic personnel training that includes technical actions

Answer: C

Explanation:

Chain of custody forms with points of contact are the best way to enable an organization to maintain legally admissible evidence because they document the sequence of control, transfer, and analysis of the evidence, and every person who handled it, the dates and times, and the purpose for each action1. They also ensure the authenticity and integrity of the evidence, and prevent tampering or loss1. Documented processes around forensic records retention are not sufficient to maintain legally admissible evidence because they do not track or verify the handling of the evidence. Robust legal framework with notes of legal actions are not sufficient to maintain legally admissible evidence because they do not record or validate the preservation of the evidence. Forensic personnel training that includes technical actions are not sufficient to maintain legally admissible evidence because they do not account or certify the custody of the evidence.
Reference: 1 https://www.researchgate.net/publication/326079761_Digital_Chain_of_Custody

Question: 338

Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS)

attack on a public-facing web server?

A. Execution of unauthorized commands
B. Prevention of authorized access
C. Defacement of website content
D. Unauthorized access to resources

Answer: B

Explanation:

Prevention of authorized access is the greatest threat posed by a distributed denial of service (DDoS) attack on a public-facing web server because it prevents legitimate users or customers from accessing the web services or resources, causing disruption, dissatisfaction, and potential loss of revenue or reputation. Execution of unauthorized commands is not a threat posed by a DDoS attack, but rather by a remote code execution (RCE) attack. Defacement of website content is not a threat posed by a DDoS attack, but rather by a web application attack. Unauthorized access to resources is not a threat posed by a DDoS attack, but rather by a brute force attack or an authentication bypass attack. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value- of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume- 5/security-scanning-versus-penetration-testing

Question: 339

Which of the following should an information security manager do FIRST when creating an organization's disaster recovery plan (DRP)?

A. Conduct a business impact analysis (BIA)
B. Identify the response and recovery learns.
C. Review the communications plan.

D. Develop response and recovery strategies.

Answer: A

Explanation:

Conducting a business impact analysis (BIA) is the first step when creating an organization's disaster recovery plan (DRP) because it helps to identify and prioritize the critical business functions or processes that need to be restored after a disruption, and determine their recovery time objectives (RTOs) and recovery point objectives (RPOs)2. Identifying the response and recovery teams is not the first step, but rather a subsequent step that involves assigning roles and responsibilities for executing the DRP. Reviewing the communications plan is not the first step, but rather a subsequent step that involves defining the communication channels and protocols for notifying and updating the stakeholders during and after a disruption. Developing response and recovery strategies is not the first step, but rather a subsequent step that involves selecting and implementing the appropriate

solutions and procedures for restoring the critical business functions or processes.
Reference: 2 https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/business- impact-analysis-bia-and-disaster-recovery-planning-drp

Question: 340

Regular vulnerability scanning on an organization's internal network has identified that many user workstations have unpatched versions of software. What is the BEST way for the information security manager to help senior management understand the related risk?

A. Include the impact of the risk as part of regular metrics.
B. Recommend the security steering committee conduct a review.
C. Update the risk assessment at regular intervals
D. Send regular notifications directly to senior managers

Answer: A

Explanation:

Including the impact of the risk as part of regular metrics is the best way for the information security manager to help senior management understand the related risk of having many user workstations with unpatched versions of software because it quantifies and communicates the potential consequences and likelihood of such a risk in terms of business objectives and performance indicators. Recommending the security steering committee conduct a review is not a good way because it does not provide any specific information or analysis about the risk or its impact. Updating the risk assessment at regular intervals is not a good way because it does not ensure that senior management is aware or informed about the risk or its impact. Sending regular notifications directly to senior managers is not a good way because it may be perceived as intrusive or annoying, and may not convey the severity or urgency of the risk or its impact. Reference: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of- information-security-investments https://www.isaca.org/resources/isaca- journal/issues/2017/volume-3/how-to-measure-

the-effectiveness-of-your-information-security- management-system

Question: 341

An incident management team leader sends out a notification that the organization has successfully recovered from a cyberattack. Which of the following should be done NEXT?

A. Prepare an executive summary for senior management
B. Gather feedback on business impact
C. Conduct a meeting to capture lessons learned.
D. Secure and preserve digital evidence for analysis.

Answer: C

Explanation:

Conducting a meeting to capture lessons learned is the next step after an incident management team leader sends out a notification that the organization has successfully recovered from a cyberattack because it helps to identify the strengths and weaknesses of the current incident response plan, capture the feedback and recommendations from the incident responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Preparing an executive summary for senior management is not the next step, but rather a subsequent step that involves reporting the incident details, impact, and resolution to the senior management. Gathering feedback on business impact is not the next step, but rather a concurrent step that involves assessing the extent and severity of the damage or disruption caused by the incident. Securing and preserving digital evidence for analysis is not the next step, but rather a previous step that involves collecting and documenting the relevant data or artifacts related to the incident. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident- response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume- 3/incident-response-lessons-learned

Question: 342

The contribution of recovery point objective (RPO) to disaster recovery is to:

A. minimize outage periods.
B. eliminate single points of failure.
C. define backup strategy
D. reduce mean time between failures (MTBF).

Answer: C

Explanation:

The contribution of recovery point objective (RPO) to disaster recovery is to define backup strategy because it determines the maximum amount of data loss that is acceptable to an organization after a disruption, and guides the frequency and type of backups needed to restore the data to a usable format1. Minimize outage

periods is not a contribution of RPO, but rather a contribution of recovery time objective (RTO), which defines the maximum amount of time that is acceptable to restore normal operations after a disruption2. Eliminate single points of failure is not a contribution of RPO, but rather a goal of high availability (HA), which ensures that systems or services are continuously operational and resilient3. Reduce mean time between failures (MTBF) is not a contribution of RPO, but rather a measure of reliability, which indicates the average time that a system or component operates without failure4. Reference: 1 https://www.druva.com/glossary/what-is-a-recovery-point- objective-definition-and-related-faqs 2 https://www.druva.com/glossary/what-is-a-recovery-time- objective-definition-and-related-faqs 3 https://www.fortinet.com/resources/cyberglossary/high-availability 4 https://www.fortinet.com/resources/cyberglossary/mean-time-between-failures

Question: 343

Senior management has just accepted the risk of noncompliance with a new regulation What should the information security manager do NEX*P

A. Report the decision to the compliance officer
B. Update details within the risk register.
C. Reassess the organization's risk tolerance.
D. Assess the impact of the regulation.

Answer: B

Explanation:

Updating details within the risk register is the next step for the information security manager to do after senior management has accepted the risk of noncompliance with a new regulation because it records and communicates the risk status, impact, and response strategy to the relevant stakeholders. Reporting the decision to the compliance officer is not the next step, but rather a possible subsequent step that involves informing and consulting with the compliance officer about the risk acceptance and its implications. Reassessing the organization's risk tolerance is not the next step, but rather a possible subsequent step that involves reviewing and adjusting the organization's risk appetite and thresholds based on the risk acceptance and its implications. Assessing the impact of the regulation is not the next step, but rather a previous step that involves analyzing and evaluating the potential consequences and likelihood of noncompliance with the regulation.
Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure- the-effectiveness-of-information-security-using-iso-27004 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

Question: 344

The PRIMARY goal of the eradication phase in an incident response process is to:

A. maintain a strict chain of custody.
B. provide effective triage and containment of the incident.
C. remove the threat and restore affected systems
D. obtain forensic evidence from the affected system.

Answer: C

Explanation:

The primary goal of the eradication phase in an incident response process is to remove the threat and restore affected systems because it eliminates any traces or remnants of malicious activity or compromise from the systems or network, and returns them to their normal or secure state.
Maintaining a strict chain of custody is not a goal of the eradication phase, but rather a requirement

for preserving and documenting digital evidence throughout the incident response process. Providing effective triage and containment of the incident is not a goal of the eradication phase, but rather a goal of the containment phase, which isolates and stops the spread of malicious activity or compromise. Obtaining forensic evidence from the affected system is not a goal of the eradication phase, but rather a goal of the identification phase, which collects and analyzes data or artifacts related to malicious activity or compromise.
Reference: https://www.isaca.org/resources/isaca- journal/issues/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

Question: 345

An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:

- A bad actor broke into a business-critical FTP server by brute forcing an administrative password
- The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
- The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
- After three hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail

Which of the following could have been prevented by conducting regular incident response testing?

A. Ignored alert messages
B. The server being compromised
C. The brute force attack
D. Stolen data

Answer: A

Explanation:

Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular

incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons- learned

Question: 346

Which of the following is the BEST option to lower the cost to implement application security controls?

A. Perform security tests in the development environment.
B. Integrate security activities within the development process
C. Perform a risk analysis after project completion.
D. Include standard application security requirements

Answer: B

Explanation:

Integrating security activities within the development process is the best option to lower the cost to implement application security controls because it ensures that security is considered and addressed throughout the software development life cycle (SDLC), from design to deployment, and reduces the likelihood and impact of security flaws or vulnerabilities that may require costly fixes or patches later on. Performing security tests in the development environment is not the best option because it may not detect or prevent all security issues that may arise in different environments or scenarios.
Performing a risk analysis after project completion is not a good option because it may be too late to identify or mitigate security risks that may have been introduced during the project. Including standard application security requirements is not a good option because it may not account for specific or unique security needs or challenges of different applications or projects. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software- development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume- 4/technical-security-standards-for-information-systems

Question: 347

Which of the following would provide the MOST effective security outcome in an organizations contract management process?

A. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage
B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage
C. Extending security assessment to cover asset disposal on contract termination
D. Extending security assessment to include random penetration testing

Answer: B

Explanation:

Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective

security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the

organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves comparing and ranking different vendors or service providers based on their security capabilities or performance. Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership- and-custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

Question: 348

Which of the following should be done FIRST when implementing a security program?

A. Perform a risk analysis
B. Implement data encryption.
C. Create an information asset inventory.
D. Determine the value of information assets.

Answer: A

Explanation:

Performing a risk analysis is the first step when implementing a security program because it helps to identify and prioritize the potential threats and vulnerabilities that may affect the organization's assets, processes, or objectives, and determine their impact and likelihood. Implementing data encryption is not the first step, but rather a possible subsequent step that involves applying a specific security control or technique to protect data from unauthorized access or modification. Creating an information asset inventory is not the first step, but rather a possible subsequent step that involves identifying and classifying the organization's assets based on their value and sensitivity. Determining the value of information assets is not the first step, but rather a possible subsequent step that involves estimating and quantifying the worth of information assets to the organization. Reference: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of- information-security-investments https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

Question: 349

Which of the following is MOST important to include in an information security status report management?

A. List of recent security events
B. Key risk indication (KRIs)

C. Review of information security policies
D. information security budget requests

Answer: B

Explanation:

Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso- 27004

Question: 350

What type of control is being implemented when a security information and event management (SIEM) system is installed?

A. Preventive
B. Deterrent
C. Detective
D. Corrective

Answer: C

Explanation:

A security information and event management (SIEM) system is a type of detective control because it monitors and analyzes the security events or logs from different sources or systems, and detects any anomalies or incidents that may indicate a security breach or compromise. A preventive control is a type of control that prevents or blocks any unauthorized or malicious activity or access from occurring. A deterrent control is a type of control that discourages or warns any potential attackers or intruders from attempting any unauthorized or malicious activity or access. A corrective control is a type of control that restores or repairs any damage or disruption caused by an unauthorized or malicious activity or access. Reference: https://www.isaca.org/resources/isaca-

journal/issues/2017/volume-6/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

Question: 351

Which of the following is MOST useful to an information security manager when determining the need to escalate an incident to senior?

A. Incident management procedures
B. Incident management policy
C. System risk assessment
D. Organizational risk register

Answer: D

Explanation:

The organizational risk register is the most useful for an information security manager when determining the need to escalate an incident to senior management because it contains a list of identified risks to the organization, their likelihood and impact, and their predefined risk thresholds or targets, which can help the information security manager assess the severity and urgency of the incident and decide whether it requires senior management's attention or action. Incident management procedures are not very useful for this purpose because they do not provide any specific criteria or guidance on when to escalate an incident to senior management. Incident management policy is not very useful for this purpose because it does not provide any specific criteria or guidance on when to escalate an incident to senior management. System risk assessment is not very useful for this purpose because it does not reflect the current risk exposure or status of the organization as a whole. Reference: https://www.isaca.org/resources/isaca- journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso- 27004 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response- lessons-learned

Question: 352

In the context of developing an information security strategy, which of the following provides the MOST useful input to determine the or

A. Security budget
B. Risk register
C. Risk score
D. Laws and regulations

Answer: D

Explanation:

Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security needs or goals, but rather a resource to enable the

security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. Reference: https://www.isaca.org/resources/isaca- journal/issues/2016/volume-4/technical-security-standards-for-information-systems https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security- initiatives-with-business-goals-and-objectives

Question: 353

An employee clicked on a link in a phishing email, triggering a ransomware attack Which of the following should be the information security?

A. Wipe the affected system.
B. Notify internal legal counsel.
C. Notify senior management.
D. Isolate the impacted endpoints.

Answer: D

Explanation:

Isolating the impacted endpoints is the best course of action for the information security manager after an employee clicked on a link in a phishing email, triggering a ransomware attack because it prevents the ransomware from spreading to other systems or devices on the network, and minimizes the damage or disruption caused by the attack. Wiping the affected system is not a good course of action because it may destroy any evidence or data that could be used for investigation or recovery. Notifying internal legal counsel is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. Notifying senior management is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident- response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume- 3/incident-response-lessons-learned

Question: 354

After a server has been attacked, which of the following is the BEST course of action?

A. Initiate incident response.
B. Review vulnerability assessment.
C. Conduct a security audit.
D. Isolate the system.

Answer: A

Explanation:

Initiating incident response is the best course of action after a server has been attacked because it activates the incident response plan or process, which defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Reviewing vulnerability assessment is not a good course of action because it does not address the current attack or its impact, but rather evaluates the potential weaknesses or exposures of the server. Conducting a security audit is not a good course of action because it does not address the current attack or its impact, but rather verifies and validates the compliance or performance of the server's security controls or systems. Isolating the system is not a good course of action because it does not address the current attack or its impact, but rather stops or limits any communication or interaction with the server. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons- learned

Question: 355

Which of the following is the GREATEST concern resulting from the lack of severity criteria in incident classification?

A. Statistical reports will be incorrect.
B. The service desk will be staffed incorrectly.
C. Escalation procedures will be ineffective.
D. Timely detection of attacks will be impossible.

Answer: C

Explanation:

The greatest concern resulting from the lack of severity criteria in incident classification is that escalation procedures will be ineffective because they rely on severity criteria to determine when and how to escalate an incident to higher levels of authority or responsibility, and what actions or resources are required for resolving an incident. Statistical reports will be incorrect is not a great concern because they do not affect the incident response process directly, but rather provide information or analysis for improvement or evaluation purposes. The service desk will be staffed incorrectly is not a great concern because it does not affect the incident response process directly,

but rather affects the availability or efficiency of one of its components. Timely detection of attacks will be impossible is not a great concern because it does not depend on severity criteria, but rather on monitoring and alerting mechanisms. Reference: https://www.isaca.org/resources/isaca- journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons- learned

Question: 356

In a call center, the BEST reason to conduct a social engineering is to:

A. Identify candidates for additional security training.
B. minimize the likelihood of successful attacks.
C. gain funding for information security initiatives.

D. improve password policy.

Answer: A

Explanation:

The best reason to conduct a social engineering test in a call center is to identify candidates for additional security training because it helps to assess the level of awareness and skills of the call center staff in recognizing and resisting social engineering attacks, and provide them with the necessary training or education to improve their security posture. Minimizing the likelihood of successful attacks is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Gaining funding for information security initiatives is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Improving password policy is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration- testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning- versus-penetration-testing

Question: 357

To ensure that a new application complies with information security policy, the BEST approach is to:

A. review the security of the application before implementation.
B. integrate functionality the development stage.
C. perform a vulnerability analysis.
D. periodically audit the security of the application.

Answer: B

Explanation:

Performing a vulnerability analysis is the best option to ensure that a new application complies with information security policy because it helps to identify and evaluate any security flaws or weaknesses in the application that may expose it to potential threats or attacks, and provide recommendations or solutions to mitigate them. Reviewing the security of the application before implementation is not a good option because it may not detect or prevent all security issues that may arise after implementation or deployment. Integrating security functionality at the development stage is not a good option because it may not account for all security requirements or challenges of the application or its environment. Periodically auditing the security of the application is not a good option because it may not address any security issues that may occur between audits or after deployment. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software-development-lifecycle https://www.isaca.org/resources/isaca- journal/issues/2016/volume-4/integrating-assurance-functions

Question: 358

An information security manager has identified that security risks are not being treated in a timely manner.

Which of the following

A. Provide regular updates about the current state of the risks.
B. Re-perform risk analysis at regular intervals.
C. Assign a risk owner to each risk
D. Create mitigating controls to manage the risks.

Answer: B

Explanation:

An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. Reference: https://support.microsoft.com/en-us/office/secure-messages-by-using- a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6
https://www.techtarget.com/searchsecurity/definition/digital-signature

Question: 359

An email digital signature will:

A. protect the confidentiality of an email message.
B. verify to recipient the integrity of an email message.
C. automatically correct unauthorized modification of an email message.
D. prevent unauthorized modification of an email message.

Answer: B

Explanation:

An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. Reference: https://support.microsoft.com/en-us/office/secure-messages-by-using- a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6
https://www.techtarget.com/searchsecurity/definition/digital-signature

Question: 360

From an information security perspective, legal issues associated with a transborder flow of technology-related items are MOST often

A. website transactions and taxation.
B. software patches and corporate date.
C. encryption tools and personal data.
D. lack of competition and free trade.

Answer: C

Explanation:

Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow. Reference: https://www.oecd-ilibrary.org/science-and-technology/oecd- declaration-on-transborder-data-flows_230240624407
https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

Question: 361

Which of the following is MOST important in order to obtain senior leadership support when presenting an information security strategy?

A. The strategy aligns with management's acceptable level of risk.
B. The strategy addresses ineffective information security controls.
C. The strategy aligns with industry benchmarks and standards.
D. The strategy addresses organizational maturity and the threat environment.

Answer: A

Explanation:

The most important factor to obtain senior leadership support when presenting an information security strategy is that the strategy aligns with management's acceptable level of risk because it ensures that the

strategy is consistent and compatible with the organization's risk appetite and thresholds, and reflects management's expectations and priorities for security risk management. The strategy addresses ineffective information security controls is not a very important factor because it does not indicate how the strategy will improve or enhance the security controls or performance. The strategy aligns with industry benchmarks and standards is not a very important factor because it does not indicate how the strategy will differentiate or innovate the organization's security capabilities or practices. The strategy addresses organizational maturity and the threat environment is not a very important factor because it does not indicate how the strategy will advance or adapt the organization's security posture or resilience. Reference: https://www.isaca.org/resources/isaca- journal/issues/2016/volume-4/technical-security-standards-for-information-systems https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security- initiatives-with-business-goals-and-objectives

Question: 362

The MOST important information for influencing management's support of information security is:

A. an demonstration of alignment with the business strategy.
B. An identification of the overall threat landscape.
C. A report of a successful attack on a competitor.
D. An identification of organizational risks.

Answer: A

Explanation:

The most important information for influencing management's support of information security is an demonstration of alignment with the business strategy because it shows how information security contributes to the achievement of the organization's goals and objectives, and adds value to the organization's performance and competitiveness. An identification of the overall threat landscape is not very important because it does not indicate how information security addresses or mitigates the threats or risks. A report of a successful attack on a competitor is not very important because it does not indicate how information security prevents or responds to such attacks. An identification of organizational risks is not very important because it does not indicate how information security manages or reduces the risks. Reference: https://www.isaca.org/resources/isaca- journal/issues/2016/volume-4/technical-security-standards-for-information-systems https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security- initiatives-with-business-goals-and-objectives

Question: 363

An investigation of a recent security incident determined that the root cause was negligent handing of incident alerts by system admit manager to address this issue?

A. Conduct a risk assessment and share the result with senior management.
B. Revise the incident response plan-to align with business processes.
C. Provide incident response training to data custodians.
D. Provide incident response training to data owners.

Answer: C

Explanation:

The best action for the system admin manager to address the issue of negligent handling of incident alerts by system admins is to provide incident response training to data custodians because it helps to improve their awareness and skills in recognizing and reporting security incidents, and following the incident response procedures and protocols. Conducting a risk assessment and sharing the result with senior management is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Revising the incident response plan to align with business processes is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Providing incident response training to data owners is not a good action because data owners are not responsible for handling incident alerts or performing incident response tasks. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume- 5/incident-response-lessons-learned https://www.isaca.org/resources/isaca- journal/issues/2018/volume-3/incident-response-lessons-learned

Question: 364

Which of the following has the GREATEST influence on the successful integration of information security within the business?

A. Organizational structure and culture
B. Risk tolerance and organizational objectives
C. The desired state of the organization
D. Information security personnel

Answer: A

Explanation:

The factor that has the greatest influence on the successful integration of information security within the business is organizational structure and culture because they determine how information security is organized, governed, and supported within the organization, and how information security roles and responsibilities are defined, assigned, and communicated across different levels and functions. Risk tolerance and organizational objectives are not very influential because they do not affect how information security is integrated within the business, but rather what information security aims to achieve or protect. The desired state of the organization is not very influential because it does not affect how information security is integrated within the business, but rather what the organization aspires to be or do. Information security personnel are not very influential because they do not affect how information security is integrated within the business, but rather who performs information security tasks or activities. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards- for-information-systems https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how- to-align-security-initiatives-with-business-goals-and-objectives

Question: 365

Which of the following BEST supports effective communication during information security incidents7

A. Frequent incident response training sessions
B. Centralized control monitoring capabilities
C. Responsibilities defined within role descriptions
D. Predetermined service level agreements (SLAs)

Answer: D

Explanation:

The best way to support effective communication during information security incidents is to have predetermined service level agreements (SLAs) because they define the expectations and responsibilities of the parties involved in the incident response process, and specify the communication channels, methods, and frequency for reporting and updating on the incident status and resolution. Frequent incident response training sessions are not very effective because they do not address the communication needs or challenges during an actual incident. Centralized control monitoring capabilities are not very effective because they do not address the communication needs

or challenges during an actual incident. Responsibilities defined within role descriptions are not very effective because they do not address the communication needs or challenges during an actual incident. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident- response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume- 3/incident-response-lessons-learned

Question: 366

Which of the following should include contact information for representatives of equipment and software vendors?

A. Information security program charter
B. Business impact analysis (BIA)
C. Service level agreements (SLAs)
D. Business continuity plan (BCP)

Answer: D

Explanation:

The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization's critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. Reference: https://www.isaca.org/resources/isaca-

journal/issues/2017/volume-2/business-continuity-management-lifecycle
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis

Question: 367

Which of the following should be triggered FIRST when unknown malware has infected an organization's critical system?

A. Incident response plan
B. Disaster recovery plan (DRP)
C. Business continuity plan (BCP)
D. Vulnerability management plan

Answer: A

Explanation:

The document that should be triggered first when unknown malware has infected an organization's critical system is the incident response plan because it defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Disaster recovery plan (DRP) is not a good document for this purpose because it focuses on restoring the organization's critical systems and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Business continuity plan (BCP) is not a good document for this purpose because it focuses on restoring the organization's critical business functions and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Vulnerability management plan is not a good document for this purpose because it focuses on identifying and evaluating the security weaknesses or exposures of the organization's systems and assets, which may not be relevant or helpful at this stage. Reference: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident- response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume- 3/incident-response-lessons-learned

Question: 368

A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by IN information security manager?

A. Determine the required security controls for the new solution
B. Review the disaster recovery plans (DRPs) of the providers
C. Obtain audit reports on the service providers' hosting environment
D. Align the roles of the organization's and the service providers' stats.

Answer: A

Explanation:

Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question: 369

Which of the following is the BEST way lo monitor for advanced persistent threats (APT) in an organization?

A. Network with peers in the industry to share information.

B. Browse the Internet to team of potential events
C. Search for anomalies in the environment
D. Search for threat signatures in the environment.

Answer: C

Explanation:

An advanced persistent threat (APT) is a stealthy and sophisticated attack that aims to compromise and maintain access to a target network or system over a long period of time, often for espionage or sabotage purposes. APTs are difficult to detect by conventional security tools, such as antivirus or firewalls, that rely on signatures or rules to identify threats. Therefore, the best way to monitor for APTs is to search for anomalies in the environment, such as unusual network traffic, user behavior, file activity, or system configuration changes, that may indicate a compromise or an ongoing attack. Reference: https://www.isaca.org/credentialing/cism https://www.nist.gov/publications/information-security-handbook-guide-managers

Question: 370

Which of the following should an information security manager do FIRST after a new cybersecunty regulation has been introduced?

A. Conduct a cost-benefit analysis.
B. Consult corporate legal counsel
C. Update the information security policy.
D. Perform a gap analysis.

Answer: D

Explanation:

When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability, and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the

potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory requirements. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question: 371

In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?

A. Ownership of security
B. Compliance with policies
C. Auditability of systems
D. Allocation of training resources

Answer: A

Explanation:

Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. In addition to executive sponsorship and business alignment, a critical factor for effective information security governance is ownership of security, which means that the roles and responsibilities for information security are clearly defined and assigned to the appropriate stakeholders, such as business owners, information owners, information custodians, and users. Ownership of security also implies accountability for the protection of information assets and the management of security risks. Reference: https://www.isaca.org/credentialing/cism https://www.nist.gov/publications/information-security- handbook-guide-managers

Question: 372

An organization is leveraging tablets to replace desktop computers shared by shift-based staff These tablets contain critical business data and are inherently at increased risk of theft Which of the following will BEST help to mitigate this risk''

A. Deploy mobile device management (MDM)
B. Implement remote wipe capability.
C. Create an acceptable use policy.
D. Conduct a mobile device risk assessment

Answer: D

Explanation:

A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should

be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p- 9781119801948

Question: 373

Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?

A. Return on investment (ROI)
B. Compliance requirements
C. Target audience
D. Criticality of information

Answer: D

Explanation:

A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. Reference: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p- 9781119801948

Question: 374

Which of the following BEST enables an organization to effectively manage emerging cyber risk?

A. Periodic internal and external audits
B. Clear lines of responsibility
C. Sufficient cyber budget allocation
D. Cybersecurity policies

Answer: D

Explanation:

Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the

foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber budget allocation

demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals. Reference: https://www.isaca.org/credentialing/cism
https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question: 375

After a recovery from a successful malware attack, instances of the malware continue to be discovered. Which phase of incident response was not successful?

A. EradicationB Recovery
B. Lessons learned review
C. Incident declaration

Answer: A

Explanation:

Eradication is the phase of incident response where the incident team removes the threat from the affected systems and restores them to a secure state. If this phase is not successful, the malware may persist or reappear on the systems, causing further damage or compromise. Therefore, eradication is the correct answer.
Reference:
https://www.securitymetrics.com/blog/6-phases-incident-response-plan
https://www.atlassian.com/incident-management/incident-response
https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life- cycle/

Question: 376

An organization has decided to outsource IT operations. Which of the following should be the PRIMARY focus of the information security manager?

A. Security requirements are included in the vendor contract
B. External security audit results are reviewed.
C. Service level agreements (SLAs) meet operational standards.
D. Business continuity contingency planning is provided

Answer: A

Explanation:

Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or

laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.

Reference:

https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity- operations

https://www.sciencedirect.com/science/article/pii/S0378720616302166

Question: 377

A penetration test against an organization's external web application shows several vulnerabilities.

Which of the following presents the GREATEST concern?

A. A rules of engagement form was not signed prior to the penetration test
B. Vulnerabilities were not found by internal tests
C. Vulnerabilities were caused by insufficient user acceptance testing (UAT)
D. Exploit code for one of the vulnerabilities is publicly available

Answer: D

Explanation:

Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.

Reference:

https://www.imperva.com/learn/application-security/penetration-testing/

https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your- web-application-for-vulnerabilities/

Question: 378

Which of the following is MOST helpful in determining the criticality of an organization's business functions?

A. Disaster recovery plan (DRP)
B. Business impact analysis (BIA)
C. Business continuity plan (BCP)
D. Security assessment report (SAR)

Answer: B

Explanation:

Business impact analysis (BIA) is the most helpful in determining the criticality of an organization's business functions because it is a process of identifying and evaluating the potential effects of disruptions or interruptions to those functions. BIA helps to prioritize the recovery of the most critical functions and to estimate the resources and time needed for the recovery. Therefore, business impact analysis (BIA) is the correct answer.

Reference:

https://www.linkedin.com/pulse/business-continuity-critical-functions-tino-marquez

https://www.techtarget.com/searchitchannel/feature/Business-impact-analysis-for-business- continuity-Understanding-impact-criticality

Question: 379

An organization has purchased an Internet sales company to extend the sales department. The information security manager's FIRST step to ensure the security policy framework encompasses the new business model is to:

A. perform a gap analysis.
B. implement both companies' policies separately
C. merge both companies' policies
D. perform a vulnerability assessment

Answer: A

Explanation:

Performing a gap analysis is the first step to ensure the security policy framework encompasses the new business model because it is a process of comparing the current state of security policies and controls with the desired or required state. A gap analysis helps to identify the strengths and weaknesses of the existing security policy framework, as well as the opportunities and threats posed by the new business model. A gap analysis also helps to prioritize the actions and resources needed to close the gaps and align the security policy framework with the new business objectives and requirements. Therefore, performing a gap analysis is the correct answer.

Reference:

https://secureframe.com/blog/security-frameworks

https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing- the-right-one

Question: 380

Following a risk assessment, an organization has made the decision to adopt a bring your own device (BYOD)

strategy. What should the information security manager do NEXT?

A. Develop a personal device policy
B. Implement a mobile device management (MDM) solution
C. Develop training specific to BYOD awareness
D. Define control requirements

Answer: D

Explanation:

Defining control requirements is the next step to ensure the security policy framework encompasses the new business model because it is a process of identifying and specifying the security measures and standards that are needed to protect the data and applications accessed by the BYOD devices. Defining control requirements helps to establish the baseline security level and expectations for the BYOD strategy, as well as to align them with the business objectives and risks. Therefore, defining control requirements is the correct answer.

Reference:

https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges- creating-effective-policies-and-mitigating

https://learn.microsoft.com/en-us/mem/intune/fundamentals/byod-technology-decisions

Question: 381

Which of the following is BEST used to determine the maturity of an information security program?

A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics

Answer: D

Explanation:

Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes. Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.

Reference:

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators- for-security-governance-part-1

https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for- maturing-

information-security

Question: 382

Which of the following is the BEST way to reduce the risk of security incidents from targeted email attacks?

A. Implement a data loss prevention (DLP) system
B. Disable all incoming cloud mail services
C. Conduct awareness training across the organization
D. Require acknowledgment of the acceptable use policy

Answer: C

Explanation:

Conducting awareness training across the organization is the best way to reduce the risk of security incidents from targeted email attacks because it helps to educate and empower the employees to recognize and avoid falling for such attacks. Targeted email attacks, such as phishing, spear phishing, or business email compromise, rely on social engineering techniques to deceive and manipulate the recipients into clicking on malicious links, opening malicious attachments, or disclosing sensitive information. Awareness training can help to raise the level of security culture and behavior among the employees, as well as to provide them with practical tips and best practices to protect themselves and the organization from targeted email attacks. Therefore, conducting awareness training across the organization is the correct answer.

Reference:

https://almanac.upenn.edu/articles/one-step-ahead-dont-get-caught-by-targeted-email-attacks
https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email- compromise-bec
https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and- techniques.html

Question: 383

When implementing a security policy for an organization handling personally identifiable information (PII); the MOST important objective should be:

A. strong encryption
B. regulatory compliance.
C. data availability.
D. security awareness training

Answer: B

Explanation:

Regulatory compliance is the most important objective when implementing a security policy for an

organization handling personally identifiable information (PII) because it helps to ensure that the organization meets the legal and ethical obligations to protect the privacy and security of PII. PII is any information that can be used to identify, contact, or locate an individual, such as name, address, email, phone number, social security number, etc. PII is subject to various laws and regulations in different jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Failing to comply with these regulations can result in fines, lawsuits, reputational damage, or loss of trust. Therefore, regulatory compliance is the correct answer.

Reference:

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en

https://www.digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss- or-compromise

https://blog.rsisecurity.com/how-to-make-a-personally-identifiable-information-policy/

Question: 384

A forensic examination of a PC is required, but the PC has been switched off. Which of the following should be done FIRST?

A. Perform a backup of the hard drive using backup utilities.
B. Perform a bit-by-bit backup of the hard disk using a write-blocking device
C. Perform a backup of the computer using the network
D. Reboot the system using third-party forensic software in the CD-ROM drive

Answer: B

Explanation:

Performing a bit-by-bit backup of the hard disk using a write-blocking device is the first step to do when a forensic examination of a PC is required, but the PC has been switched off because it helps to create a forensically sound copy of the original evidence without altering or damaging it. A bit-by-bit backup, also known as a physical or raw image, is a complete copy of every bit on the hard disk, including the unallocated or deleted data. A write-blocking device is a hardware or software tool that prevents any write operations to the hard disk, such as updating timestamps or changing file attributes. Performing a bit-by-bit backup of the hard disk using a write-blocking device ensures the integrity and authenticity of the evidence and allows the forensic analysis to be conducted on the duplicate image rather than the original source. Therefore, performing a bit-by-bit backup of the hard disk using a write-blocking device is the correct answer.

Reference:

https://en.wikipedia.org/wiki/Computer_forensics

https://resources.infosecinstitute.com/topic/computer-forensics-forensic-analysis-examination- planning/

https://www.computer-forensics-recruiter.com/topics/examination_steps/

Question: 385

Which of the following is the BEST defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns?

A. Compartmentalization
B. Overlapping redundancy
C. Continuous monitoring
D. Multi-factor authentication

Answer: A

Explanation:

Compartmentalization is the best defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns because it is a strategy that divides the network or system into smaller segments or compartments, each with its own security policies, controls, and access rules. Compartmentalization helps to isolate and protect the most sensitive or critical data and functions from unauthorized or malicious access, as well as to limit the damage or impact of a breach or compromise. Compartmentalization also helps to enforce the principle of least privilege, which grants users or processes only the minimum access rights they need to perform their tasks. Therefore, compartmentalization is the correct answer.

Reference:
https://www.csoonline.com/article/3667476/defense-in-depth-explained-layering-tools-and- processes-for-better-security.html
https://www.fortinet.com/resources/cyberglossary/defense-in-depth
https://sciencepublishinggroup.com/journal/paperinfo?journalid=542&doi=10.11648/j.ajai.2019030 2.11

Question: 386

Which of the following is MOST important to have in place for an organization's information security program to be effective?

A. Documented information security processes
B. A comprehensive IT strategy
C. Senior management support
D. Defined and allocated budget

Answer: C

Explanation:

Senior management support is the most important factor to have in place for an organization’s information security program to be effective because it helps to establish the vision, direction, and goals of the program, as well as to allocate the necessary resources and authority to implement and maintain it. Senior management support also helps to foster a security culture within the organization, where security is seen as a shared responsibility and a business enabler. Senior management support also helps to ensure compliance with internal and external security policies and standards, as well as to communicate the value and impact of security to stakeholders. Therefore, senior management support is the correct answer.

Reference:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators- for-security-governance-part-1
https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdfhttps://www.cdse.edu/Portals/124/Documents/student-guides/IF011- guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d

Question: 387

While responding to a high-profile security incident, an information security manager observed several deficiencies in the current incident response plan. When would be the BEST time to update the plan?

A. While responding to the incident
B. During a tabletop exercise
C. During post-incident review
D. After a risk reassessment

Answer: C

Explanation:

During post-incident review is the best time to update the incident response plan after observing several deficiencies in the current plan while responding to a high-profile security incident. A postincident review is a process of analyzing and evaluating the incident response activities, identifying the lessons learned, and documenting the recommendations and action items for improvement. Updating the incident response plan during post-incident review helps to ensure that the plan reflects the current best practices, addresses the gaps and weaknesses, and incorporates the feedback and suggestions from the incident response team and other stakeholders. Therefore, during post-incident review is the correct answer.

Reference:
https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdfhttps://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan
https://www.integrify.com/blog/posts/incident-response-plan-need-an-update/

Question: 388

Which of the following BEST enables the assignment of risk and control ownership?

A. Aligning to an industry-recognized control framework
B. Adopting a risk management framework
C. Obtaining senior management buy-in
D. Developing an information security strategy

Answer: C

Explanation:

Obtaining senior management buy-in is the best way to enable the assignment of risk and control ownership because it helps to establish the authority and accountability of the risk and control owners, as well as to provide them with the necessary resources and support to perform their roles. Risk and control ownership refers to the assignment of specific responsibilities and accountabilities for managing risks and controls to individuals or groups within the organization. Obtaining senior management buy-in helps to ensure that risk and control ownership is aligned with the organizational objectives, structure, and culture, as well as to communicate the expectations and benefits of risk and control ownership to all stakeholders. Therefore, obtaining senior management buy-in is the correct answer.

Reference:

https://www.protechtgroup.com/en-au/blog/risk-control-management

https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/23_getting_risk_ownership_right.ashx

https://www.linkedin.com/pulse/risk-controls-who-owns-them-david-tattam

Question: 389

Which of the following metrics is MOST appropriate for evaluating the incident notification process?

A. Average total cost of downtime per reported incident
B. Elapsed time between response and resolution
C. Average number of incidents per reporting period
D. Elapsed time between detection, reporting, and response

Answer: D

Explanation:

Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.

Reference:

https://www.atlassian.com/incident-management/kpis/common-metrics

https://securityscorecard.com/blog/how-to-use-incident-response-metrics/

https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Question: 390

Which of the following would BEST support the business case for an increase in the information security budget?

A. Cost-benefit analysis results
B. Comparison of information security budgets with peer organizations
C. Business impact analysis (BIA) results
D. Frequency of information security incidents

Answer: A

Explanation:

Cost-benefit analysis results are the best way to support the business case for an increase in the information security budget because they help to demonstrate the value and return on investment of the proposed security initiatives or projects. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or options, taking into account both quantitative and qualitative factors. A cost-benefit analysis helps to justify the need and feasibility of the security budget, as well as to prioritize the security spending based on the expected outcomes and impacts. Therefore, cost-benefit analysis results are the correct answer.

Reference:
https://www.cisa.gov/resources-tools/resources/business-case-security
https://www.cisa.gov/resources-tools/resources/isc-best-practices-making-business-case-security
https://risk3sixty.com/2020/09/21/how-to-build-a-business-case-for-security-initiatives-part-4/

Question: 391

Which of the following would BEST enable the timely execution of an incident response plan?

A. The introduction of a decision support tool B. Definition of trigger events

C. Clearly defined data classification process D. Centralized service desk

Answer: B

Explanation:

Definition of trigger events is the best way to enable the timely execution of an incident response plan because it helps to specify the conditions or criteria that initiate the incident response process. Trigger events are predefined scenarios or indicators that signal the occurrence or potential occurrence of a security incident, such as a ransomware attack, a data breach, a denial-of-service attack, or an unauthorized access attempt. Definition of trigger events helps to ensure that the incident response team is alerted and activated as soon as possible, as well as to determine the appropriate level and scope of response based on the severity and impact

of the incident. Therefore, definition of trigger events is the correct answer.

Reference:

https://www.atlassian.com/incident-management/kpis/common-metrics

https://www.varonis.com/blog/incident-response-plan/

https://holierthantao.com/2023/05/03/minimizing-disruptions-a-comprehensive-guide-to-incident-response-planning-and-execution/

Question: 392

Spoofing should be prevented because it may be used to:

A. gain illegal entry to a secure system by faking the sender's address,
B. predict which way a program will branch when an option is presented
C. assemble information, track traffic, and identify network vulnerabilities.
D. capture information such as passwords traveling through the network

Answer: A

Explanation:

Gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented. Spoofing is a technique that involves impersonating someone or something else to deceive or manipulate the recipient or target. Spoofing can be applied to various communication channels, such as emails, websites, phone calls, IP addresses, or DNS servers. One of the common goals of spoofing is to gain unauthorized access to a secure system by faking the sender's address, such as an email address or an IP address. For example, an attacker may spoof an email address of a trusted person or organization and send a phishing email that contains a malicious link or attachment. If the recipient clicks on the link or opens the attachment, they may be redirected to a fake website that asks for their credentials or downloads malware onto their device.

Alternatively, an attacker may spoof an IP address of a trusted source and send packets to a secure

system that contains malicious code or commands. If the system accepts the packets as legitimate, it may execute the code or commands and compromise its security. Therefore, gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented.

Reference:

https://www.kaspersky.com/resource-center/definitions/spoofing

https://www.cisa.gov/resources-tools/resources/business-case-security https://www.avast.com/c-spoofing

Question: 393

The PRIMARY consideration when responding to a ransomware attack should be to ensure:

A. backups are available.
B. the most recent patches have been applied.

C. the ransomware attack is contained
D. the business can operate

Answer: D

Explanation:

Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.

Reference:
https://www.cisa.gov/stopransomware/ransomware-guide
https://csrc.nist.gov/Projects/ransomware-protection-and-response
https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond

Question: 394

An information security team is planning a security assessment of an existing vendor. Which of the following approaches is MOST helpful for properly scoping the assessment?

A. Focus the review on the infrastructure with the highest risk
B. Review controls listed in the vendor contract
C. Determine whether the vendor follows the selected security framework rules
D. Review the vendor's security policy

Answer: D

Explanation:

Reviewing controls listed in the vendor contract is the most helpful approach for properly scoping the security assessment of an existing vendor because it helps to determine the security requirements and expectations that the vendor has agreed to meet. A vendor contract is a legal document that defines the terms and conditions of the business relationship between the organization and the vendor, including the scope, deliverables, responsibilities, and obligations of both parties. A vendor contract should also specify the security controls that the vendor must implement and maintain to protect the organization's data and systems, such as encryption, authentication, access control, backup, monitoring, auditing, etc. Reviewing controls listed in the vendor contract helps to ensure that the security assessment covers all the relevant aspects of the vendor's security posture, as well as to identify any gaps or discrepancies between the contract and the actual practices. Therefore, reviewing controls listed in the vendor contract is the correct answer.

Reference:
https://medstack.co/blog/vendor-security-assessments-understanding-the-basics/https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf
https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment

Question: 395

An organization has multiple data repositories across different departments. The information security manager has been tasked with creating an enterprise strategy for protecting dat a. Which of the following information security initiatives should be the HIGHEST priority for the organization?

A. Data masking
B. Data retention strategy
C. Data encryption standards
D. Data loss prevention (DLP)

Answer: C

Explanation:

Data encryption standards are the best information security initiative for creating an enterprise strategy for protecting data across multiple data repositories and different departments because they help to ensure the confidentiality, integrity, and availability of data in transit and at rest. Data encryption is a process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can access and decrypt it. Data encryption standards are the rules or specifications that define how data encryption should be performed, such as the type, strength, and mode of encryption, the key management and distribution methods, and the compliance requirements. Data encryption standards help to protect data from unauthorized access, modification, or theft, as well as to meet the regulatory obligations for data privacy and security.

Therefore, data encryption standards are the correct answer.

Reference:

https://www.techtarget.com/searchdatabackup/tip/20-keys-to-a-successful-enterprise-data- protection-strategy

https://cloudian.com/guides/data-protection/data-protection-strategy-10-components-of-an- effective-strategy/

https://www.veritas.com/information-center/enterprise-data-protection

Question: 396

Which of the following would be an information security managers PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?

A. Mobile application control
B. Inconsistent device security
C. Configuration management
D. End user acceptance

Answer: B

Explanation:

Inconsistent device security is the primary challenge for an information security manager when deploying a bring your own device (BYOD) mobile program in an enterprise because it increases the risk of data breaches and compromises. A BYOD mobile program allows employees to use their personal devices, such as smartphones, tablets, or laptops, to access the organization's network, applications, and data. However, personal devices may have different operating systems, versions, configurations, and security settings than the organization's standard devices. Moreover, personal devices may not be updated regularly, may have unauthorized or malicious apps installed, or may not have adequate protection against malware or theft. Inconsistent device security makes it difficult for the information security manager to enforce and monitor the security policies and controls across all devices, as well as to ensure compliance with the regulatory requirements for data privacy and security. Therefore, inconsistent device security is the correct answer.

Reference:
https://simplemdm.com/blog/challenges-of-bring-your-own-device-byod-policy/ https://www.timedoctor.com/blog/byod-pros-and-cons/ https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf

Question: 397

Which of the following would provide the BEST evidence to senior management that security control performance has improved?

A. Demonstrated return on security investment

B. Reduction in inherent risk
C. Results of an emerging threat analysis
D. Review of security metrics trends

Answer: D

Explanation:

Review of security metrics trends is the best evidence to senior management that security control performance has improved because it helps to measure and demonstrate the effectiveness and efficiency of the security controls over time. Security metrics are quantitative or qualitative indicators that provide information about the security status or performance of an organization, system, process, or activity. Security metrics can be used to evaluate the implementation, operation, and outcome of security controls, such as the number of vulnerabilities detected and remediated, the time to respond and recover from incidents, the compliance level with security policies and standards, or the return on security investment. Review of security metrics trends helps to identify and communicate the progress, achievements, and challenges of the security program, as well as to support decision making and continuous improvement. Therefore, review of security metrics trends is the correct answer.

Reference:

https://www.bitsight.com/blog/importance-continuous-improvement-security-performance- management
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators- for-security-governance-part-2
https://www.nist.gov/news-events/news/2021/09/dhs-nist-coordinate-releasing-preliminary- cybersecurity-performance-goals.

Question: 398

Which of the following is MOST important when defining how an information security budget should be allocated?

A. Regulatory compliance standards
B. Information security strategy
C. Information security policy
D. Business impact assessment

Answer: B

Explanation:

Information security strategy is the most important factor when defining how an information security budget should be allocated because it helps to align the security objectives and initiatives with the business goals and priorities. An information security strategy is a high-level plan that defines the

vision, mission, scope, and direction of the security program, as well as the roles and responsibilities, governance structures, policies and standards, risk management approaches, and performance measurement methods. An information security strategy helps to identify and prioritize the security needs and requirements of the organization, as well as to allocate the resources and funding accordingly. An information security strategy also helps to communicate the value and benefits of security to the stakeholders and justify the security investments. Therefore, information security strategy is the correct answer.

Reference:
https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best- practices
https://www.csoonline.com/article/3671108/how-2023-cybersecurity-budget-allocations-are- shaping-up.html
https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

Question: 399

An information security manager is working to incorporate media communication procedures into the security incident communication plan. It would be MOST important to include:

A. a directory of approved local media contacts
B. pre-prepared media statements
C. procedures to contact law enforcement

D. a single point of contact within the organization

Answer: D

Explanation:

A single point of contact within the organization is the most important element to include when incorporating media communication procedures into the security incident communication plan because it helps to ensure a consistent and accurate message to the public and avoid confusion or misinformation. A single point of contact is a designated person who is authorized and trained to communicate with the media on behalf of the organization during a security incident. The single point of contact should coordinate with the incident response team, senior management, legal counsel, and public relations to prepare and deliver timely and appropriate statements to the media, as well as to respond to any inquiries or requests. A single point of contact also helps to prevent unauthorized or conflicting disclosures from other employees or stakeholders that may harm the organization's reputation or legal position. Therefore, a single point of contact within the organization is the correct answer.

Reference:

https://www.lifars.com/2020/09/communication-during-incident-response/ https://ifpo.org/resource-links/articles-and-reports/public-and-media-relations/planning-for- effective-media-relations-during-a-critical-incident/

https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a- communication-plan.

Question: 400

Which of the following is the PRIMARY benefit of an information security awareness training program?

A. Influencing human behavior
B. Evaluating organizational security culture
C. Defining risk accountability
D. Enforcing security policy

Answer: A

Explanation:

Influencing human behavior is the primary benefit of an information security awareness training program because it helps to reduce the human errors and vulnerabilities that can compromise the security of data and systems. An information security awareness training program is a process or a program that informs and empowers users to protect data and computing assets from security risks and cyberattacks. It includes educational offerings that cover regulatory requirements, compliance policies, and safe computing practices. An information security awareness training program helps to influence human behavior by raising awareness of the security threats and challenges, enhancing knowledge and skills of the security best practices and controls, and fostering a positive security culture and attitude among the users. By influencing human behavior, an information security awareness training program can improve the security posture and performance of the organization, as well as prevent or mitigate the impact of security incidents. Therefore, influencing human

behavior is the correct answer.

Reference:

https://www.isms.online/iso-27002/control-6-3-information-security-awareness-education-and- training/ https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information- security-and-privacy-awareness-training-programs https://threatcop.com/blog/benefits-and-purpose-of-security-awareness-training/.

Question: 401

A business requires a legacy version of an application to operate but the application cannot be patched. To limit the risk exposure to the business, a firewall is implemented in front of the legacy application. Which risk treatment option has been applied?

A. Mitigate
B. Accept
C. Transfer
D. Avoid

Answer: A

Explanation:

Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures. A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched. Therefore, mitigate is the correct answer. Reference:

https://simplicable.com/risk/risk-treatment

https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management- inventory/rm-process/risk-treatment.

Question: 402

Which of the following is a viable containment strategy for a distributed denial of service (DDoS) attack?

A. Block IP addresses used by the attacker
B. Redirect the attacker's traffic
C. Disable firewall ports exploited by the attacker.
D. Power off affected servers

Answer: B

Explanation:

Redirecting the attacker's traffic is a viable containment strategy for a distributed denial of service (DDoS) attack because it helps to divert the malicious traffic away from the target server and reduce the impact of the attack. A DDoS attack is an attempt by attackers to overwhelm a server or a network with a large volume of requests or packets, preventing legitimate users from accessing the service or resource. Redirecting the attacker's traffic is a technique that involves changing the DNS settings or routing tables to send the attacker's traffic to another destination, such as a sinkhole, a honeypot, or a scrubbing center. A sinkhole is a server that absorbs and discards the malicious traffic. A honeypot is a decoy server that mimics the target server and collects information about the attacker's behavior and techniques. A scrubbing center is a service that filters out the malicious traffic and forwards only the legitimate traffic to the target server. Redirecting the attacker's traffic helps to contain the DDoS attack by reducing the load on the target server and preserving its availability and performance. Therefore, redirecting the attacker's traffic is the correct answer. Reference:

https://www.fortinet.com/resources/cyberglossary/implement-ddos-mitigation-strategy
https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-response-strategy
https://www.cloudflare.com/learning/ddos/glossary/sinkholing/.

Question: 403

Which of the following is the BEST way to determine if an information security profile is aligned with business requirements?

A. Review the key performance indicator (KPI) dashboard
B. Review security-related key risk indicators (KRIs)
C. Review control self-assessment (CSA) results
D. Review periodic security audits

Answer: B

Explanation:

Security-related KRIs are metrics that measure the effectiveness of the information security profile in achieving the business objectives and managing the risks. Reviewing security-related KRIs can help to determine if the information security profile is aligned with business requirements, as they reflect the security performance and outcomes that are relevant for the business. Reviewing other options, such as KPIs, CSAs, or audits, may provide some insights into the security status, but they are not the best way to assess the alignment with business requirements, as they may not capture the business context and goals adequately. Reference: https://www.nist.gov/cyberframework/examples-framework-profiles https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/accountability-for- information-security-roles-and-responsibilities-part-1 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security- architecturea-top-down-approach

Question: 404

Which of the following is the GREATEST challenge with assessing emerging risk in an organization?

A. Lack of a risk framework
B. Ineffective security controls
C. Presence of known vulnerabilities
D. Incomplete identification of threats

Answer: D

Explanation:

The greatest challenge with assessing emerging risk in an organization is the incomplete identification of threats, as emerging risks are often new, unknown, or unfamiliar, and may not be fully understood or assessed. Incomplete identification of threats can lead to gaps in risk analysis and management, and expose the organization to unexpected or unprepared scenarios. The other options, such as lack of a risk framework, ineffective security controls, or presence of known vulnerabilities, are not specific to emerging risks, and may apply to any type of risk assessment. Reference: https://committee.iso.org/sites/tc262/home/projects/ongoing/iso-31022-guidelines-for-impl-2.htmlhttps://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-6/emerging- risk-analysis
https://projectriskcoach.com/emerging-risks/

Question: 405

Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?

A. Demonstrating the program's value to the organization
B. Discussing governance programs found in similar organizations
C. Providing the results of external audits
D. Providing examples of information security incidents within the organization

Answer: A

Explanation:

The best way to obtain senior management support for an information security governance program is to demonstrate the program’s value to the organization, such as how it can help achieve business objectives, reduce operational risks, enhance resilience, and comply with regulations. Demonstrating the value of information security governance can help senior management understand the benefits and costs of the program, and motivate them to participate in the decision-making process. The other options, such as discussing governance programs in similar organizations, providing external audit results, or providing

examples of incidents, may not be sufficient or persuasive enough to obtain senior management support, as they may not reflect the specific needs and goals of the organization. Reference: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior- management-in-the-information-security-governance-process https://www.sans.org/white-papers/992/ https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-get-management-support-for- your-security-program.html

Question: 406

An organization has introduced a new bring your own device (BYOD) program. The security manager has determined that a small number of employees are utilizing free cloud storage services to store company data through their mobile devices. Which of the following is the MOST effective course of action?

A. Allow the practice to continue temporarily for monitoring purposes.
B. Disable the employees' remote access to company email and data
C. Initiate remote wipe of the devices
D. Assess the business need to provide a secure solution

Answer: D

Explanation:

The most effective course of action when employees are using free cloud storage services to store company data through their mobile devices is to assess the business need to provide a secure solution, such as a corporate-approved cloud service or a virtual desktop environment. Assessing the business need can help understand why employees are using free cloud storage services, what kind of data they are storing, and what are the security risks and requirements. Based on the assessment, the security manager can propose a secure solution that meets the business needs and complies with the BYOD policy. The other options, such as allowing the practice to continue, disabling remote access, or initiating remote wipe, may not address the underlying business need or may cause disruption or data loss. Reference: https://www.digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing- breach https://news.microsoft.com/en-xm/2021/03/18/how-to-have-secure-remote-working-with-a-byod- policy/ https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide- bring-your-own-device-byod

Question: 407

An employee of an organization has reported losing a smartphone that contains sensitive information The BEST step to address this situation is to:

A. disable the user's access to corporate resources.
B. terminate the device connectivity.
C. remotely wipe the device

D. escalate to the user's management

Answer: C

Explanation:

The best step to address the situation of losing a smartphone that contains sensitive information is to remotely wipe the device, which means erasing all the data on the device and restoring it to factory settings. Remotely wiping the device can prevent unauthorized access to the sensitive information and protect the organization from data breaches or leaks. Remotely wiping the device can be done through services such as Find My Device for Android or Find My iPhone for iOS, or through mobile device management (MDM) solutions. The other options, such as disabling the user's access, terminating the device connectivity, or escalating to the user's management, may not be effective or timely enough to secure the sensitive information on the device.
Reference: https://www.security.org/resources/protect-data-lost-device/
https://support.google.com/android/answer/6160491?hl=en https://www.pcmag.com/how-to/locate-lock-erase-how-to-find-lost-android-phone

Question: 408

Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?

A. Suspend the data exchange with the provider
B. Notify appropriate regulatory authorities of the breach.
C. Initiate the business continuity plan (BCP)
D. Validate the breach with the provider

Answer: D

Explanation:

The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider. Reference:
https://www.wired.com/story/sequoia-hr-data-breach/
https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware- warns-of-a-long-outage/
https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117-p599mr

Question: 409

Which of the following MUST be established to maintain an effective information security governance framework?

A. Security controls automation
B. Defined security metrics
C. Change management processes
D. Security policy provisions

Answer: D

Explanation:

Security policy provisions are the statements or rules that define the information security objectives, principles, roles and responsibilities, and requirements for the organization. Security policy provisions must be established to maintain an effective information security governance framework, as they provide the foundation and direction for the information security activities and processes within the organization. Security policy provisions also help to align the information security governance framework with the business strategy and objectives, and ensure compliance with relevant laws and regulations. The other options, such as security controls automation, defined security metrics, or change management processes, are important components of an information security governance framework, but they are not essential to establish it. Reference: https://www.iso.org/standard/74046.htmlhttps://www.nistf.gov/cyberframework https://www.iso.org/standard/27001

Question: 410

An incident response team has established that an application has been breached. Which of the following should be done NEXT?

A. Maintain the affected systems in a forensically acceptable state
B. Conduct a risk assessment on the affected application
C. Inform senior management of the breach.
D. Isolate the impacted systems from the rest of the network

Answer: D

Explanation:

The next thing an incident response team should do after establishing that an application has been breached is to isolate the impacted systems from the rest of the network, which means disconnecting them from the internet or other network connections to prevent further spread of the attack or data exfiltration. Isolating the impacted systems can help to contain the breach and limit its

impact on the organization. The other options, such as maintaining the affected systems in a forensically acceptable state, conducting a risk assessment, or informing senior management, may be done later in the incident response process, after isolating the impacted systems. Reference: https://www.crowdstrike.com/cybersecurity-101/incident-response/ https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks https://www.invicti.com/blog/web-security/incident-response-steps-web-application-security/

Question: 411

An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?

A. Lack of availability
B. Lack of accountability
C. Improper authorization
D. Inadequate authentication

Answer: B

Explanation:

The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. Reference: https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

Question: 412

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager?

A. Managing the impact
B. Identifying unacceptable risk levels
C. Assessing vulnerabilities
D. Evaluating potential threats

Answer: A

Explanation:

When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. Reference: https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/ https://www.osha.gov/safety-management/hazard-prevention https://www.cdc.gov/niosh/topics/hierarchy/default.html

Question: 413

When assigning a risk owner, the MOST important consideration is to ensure the owner has:

A. adequate knowledge of risk treatment and related control activities.
B. decision-making authority and the ability to allocate resources for risk.
C. sufficient time for monitoring and managing the risk effectively.
D. risk communication and reporting skills to enable decision-making.

Answer: B

Explanation:

Comprehensive and Detailed Explanation = The risk owner is the person or entity with the accountability and authority to manage a risk. The risk owner should have the decision-making authority and the ability to allocate resources for risk treatment and related control activities. The risk owner should also be responsible for monitoring and reporting on the risk, but these are not the most important considerations when assigning a risk owner. The risk owner may not have adequate knowledge of risk treatment and related control activities, but can delegate or consult with experts as needed. The risk owner should also have sufficient time for managing the risk effectively, but this is not a prerequisite for assigning a risk owner.

Reference =
CISM Review Manual 15th Edition, page 76
CISM Practice Quiz, question 4171

Question: 414

The MOST useful technique for maintaining management support for the information security program is:

A. informing management about the security of business operations.
B. implementing a comprehensive security awareness and training program.
C. identifying the risks and consequences of failure to comply with standards.

D. benchmarking the security programs of comparable organizations.

Answer: C

Explanation:

= According to the CISM Review Manual, one of the key success factors for an information security program is to maintain management support and commitment. This can be achieved by providing regular reports to management on the security status of the organization, the effectiveness of the security controls, and the alignment of the security program with the business objectives and strategy. By informing management about the security of business operations, the information security manager can demonstrate the value and benefits of the security program, and ensure that management is aware of the security risks and issues that need to be addressed. This technique can also help to build trust and confidence between the information security manager and the senior management, and foster a culture of security within the organization1

The other options are not as effective as informing management about the security of business operations. Implementing a comprehensive security awareness and training program is important, but it is mainly targeted at the end users and staff, not the senior management. Identifying the risks and consequences of failure to comply with standards can help to justify the need for security controls, but it can also create a negative impression of the security program as being too restrictive or punitive. Benchmarking the security programs of comparable organizations can provide some insights and best practices, but it may not reflect the specific needs and context of the organization, and it may not be relevant or applicable to the management's expectations and priorities1 Reference = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 28-29…

Question: 415

Which of the following BEST facilitates the reporting of useful information about the effectiveness of the information security program?

A. Risk heat map.
B. Security benchmark report.
C. Security metrics dashboard.
D. Key risk indicators (KRIs).

Answer: C

Explanation:

A security metrics dashboard is a graphical representation of key performance indicators (KPIs) and

key risk indicators (KRIs) that provide useful information about the effectiveness of the information security program. A security metrics dashboard can help communicate the value and performance of the information security program to senior management and other stakeholders, as well as identify areas for improvement and alignment with business objectives. A security metrics dashboard should be concise, relevant, timely, accurate, and actionable.

Reference = CISM Review Manual 16th Edition, page 163; CISM Review Questions, Answers & Explanations

Manual 9th Edition, page 419.

Question: 416

After a ransomware incident an organization's systems were restored. Which of the following should be of MOST concern to the information security manager?

A. The service level agreement (SLA) was not met.
B. The recovery time objective (RTO) was not met.
C. The root cause was not identified.
D. Notification to stakeholders was delayed.

Answer: C

Explanation:

= After a ransomware incident, the most important concern for the information security manager is to identify the root cause of the incident and prevent it from happening again. The root cause analysis (RCA) is a systematic process of finding and eliminating the underlying factors that led to the incident, such as vulnerabilities, misconfigurations, human errors, or malicious actions. Without performing a RCA, the organization may not be able to address the root cause and may face the same or similar incidents in the future, which could result in more damage, costs, and reputational loss. Therefore, the information security manager should prioritize the RCA over other concerns, such as meeting the SLA, RTO, or notification requirements, which are important but secondary to the RCA. Reference = CISM Review Manual 15th Edition, page 254-2551; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 4202

Question: 417

Management of a financial institution accepted an operational risk that consequently led to the temporary deactivation to a critical monitoring process. Which of the following should be the information security manager's GREATEST concern with this situation?

A. Impact on compliance risk.
B. Inability to determine short-term impact.
C. Impact on the risk culture.
D. Deviation from risk management best practices

Answer: C

Explanation:

Comprehensive and Detailed Explanation = The impact on the risk culture is the greatest concern for the information security manager, because it reflects the attitude and behavior of the organization towards risk management. If management accepts an operational risk that compromises a critical monitoring process, it may indicate a lack of awareness, commitment, or accountability for risk management. This may erode the

trust and confidence of the stakeholders, regulators, and customers, and expose the organization to further risks. The impact on compliance risk, the inability to determine short-term impact, and the deviation from risk management best practices are also important, but they are secondary to the impact on the risk culture.

Reference = CISM Review Manual 15th Edition, page 48. CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question ID 421.

Question: 418

To improve the efficiency of the development of a new software application, security requirements should be defined:

A. based on code review.
B. based on available security assessment tools.
C. after functional requirements.
D. concurrently with other requirements.

Answer: D

Explanation:

Security requirements should be defined concurrently with other requirements to ensure that security is built into the software development process from the beginning and not added as an afterthought. This will also improve the efficiency of the development process by reducing the need for rework and testing. Security requirements should be based on the business objectives, risk assessment, and security policies of the organization, not on code review, security assessment tools, or functional requirements. Reference = CISM Review Manual 15th Edition, page 1241; CISM Item Development Guide, page 62

Question: 419

An information security manager is MOST likely to obtain approval for a new security project when the business case provides evidence of:

A. organizational alignment
B. IT strategy alignment
C. threats to the organization
D. existing control costs

Answer: A

Explanation:

A new security project is more likely to be approved if it aligns with the organization's goals, objectives, and strategies. This shows that the project supports the business needs and adds value to the organization. Organizational alignment is one of the key elements of a business case for information security, as stated in the CISM Review Manual, 16th Edition1, page 41. IT strategy alignment, threats to the organization, and existing

control costs are also important factors to consider, but they are not as persuasive as organizational alignment in obtaining approval for a new security project. Reference = 1: CISM Review Manual, 16th Edition by Isaca (Author)

Learn more:

1. isaca.org2. amazon.com3. gov.uk

Question: 420

Which of the following is the PRIMARY role of the information security manager in application development?

A. To ensure security is integrated into the system development life cycle (SDLC)
B. To ensure compliance with industry best practice
C. To ensure enterprise security controls are implemented
D. To ensure control procedures address business risk

Answer: A

Explanation:

According to the CISM Review Manual, one of the primary roles of the information security manager in application development is to ensure that security is integrated into the SDLC. This means that security requirements, design, testing, deployment, and maintenance are all considered and addressed throughout the application development process. By doing so, the information security manager can help to prevent or mitigate security risks, ensure compliance with standards and regulations, and improve the quality and reliability of the application1

The other options are not as accurate as ensuring security is integrated into the SDLC. Ensuring compliance with industry best practices is a secondary role of the information security manager in application development, as it involves following established guidelines and frameworks for secure application development. However, compliance alone does not guarantee that security is actually implemented in the application. Ensuring enterprise security controls are implemented is a tertiary role of the information security manager in application development, as it involves applying existing policies and procedures for managing and monitoring security activities across the organization. However, enterprise controls alone do not ensure that security is tailored to the specific needs and context of each application. Ensuring control procedures address business risk is a quaternary role of the information security manager in application development, as it involves identifying and assessing potential threats and vulnerabilities that could affect the business objectives and operations of each application. However, business risk alone does not ensure that security measures are aligned with the value proposition and benefits of each application1

Reference = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 30-31…

Question: 421

Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?

A. Alignment with industry benchmarks

B. Results of business impact analyses (BIAs)
C. Possibility of reputational loss due to incidents
D. Availability of security budget

Answer: B

Explanation:

The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. Reference = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

Question: 422

Which of the following BEST minimizes information security risk in deploying applications to the production environment?

A. Integrating security controls in each phase of the life cycle
B. Conducting penetration testing post implementation
C. Having a well-defined change process
D. Verifying security during the testing process

Answer: A

Explanation:

= Integrating security controls in each phase of the life cycle is the best way to minimize information security risk in deploying applications to the production environment. This ensures that security requirements are defined, designed, implemented, tested, and maintained throughout the development process. Conducting penetration testing post implementation, having a well-defined

change process, and verifying security during the testing process are all important activities, but they are not sufficient to address all the potential risks that may arise during the application life cycle. Penetration testing may reveal some vulnerabilities, but it cannot guarantee that all of them are identified and fixed. A change process may help to control and document the modifications made to the application, but it does not ensure that the changes are secure and do not introduce new risks. Verifying security during the testing process may help to validate the functionality and performance of the security controls, but it does not ensure that the security requirements are complete and consistent with the business objectives and the risk appetite of the organization. Reference = CISM Review Manual, 16th Edition, page 1121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462

Question: 423

Which of the following is the BEST way to determine the effectiveness of an incident response plan?

A. Reviewing previous audit reports
B. Conducting a tabletop exercise
C. Benchmarking the plan against best practices
D. Performing a penetration test

Answer: B

Explanation:

A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

Question: 424

The PRIMARY goal to a post-incident review should be to:

A. identify policy changes to prevent a recurrence.
B. determine how to improve the incident handling process.
C. establish the cost of the incident to the business.
D. determine why the incident occurred.

Answer: B

Explanation:

The primary goal of a post-incident review is to identify areas for improvement in the incident handling process. The focus is on evaluating the effectiveness of incident response procedures, technical controls, communication channels, coordination among teams, documentation, and any other relevant aspects. The post-incident review should also provide recommendations for corrective actions, preventive measures, and lessons learned that can help reduce the likelihood and impact of future incidents12. Reference = CISM Review Manual 15th Edition, page 1251; CISM Item Development Guide, page 72

Question: 425

A security incident has been reported within an organization When should an information security manager contact the information owner?

A. After the incident has been mitigated

B. After the incident has been confirmed.
C. After the potential incident has been togged
D. After the incident has been contained

Answer: B

Explanation:

= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated. The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention. Reference = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

Question: 426

Which of the following is the BEST way to contain an SQL injection attack that has been detected by a web application firewall?

A. Force password changes on the SQL database.
B. Reconfigure the web application firewall to block the attack.
C. Update the detection patterns on the web application firewall.
D. Block the IPs from where the attack originates.

Answer: B

Explanation:

According to the CISM Review Manual, one of the best ways to contain an SQL injection attack that has been detected by a web application firewall is to reconfigure the web application firewall to block the attack. This means that the web application firewall should be updated with the latest detection patterns and rules that can identify and prevent SQL injection attacks. By doing so, the web application firewall can reduce the impact and damage of the attack, and prevent further exploitation of the vulnerable database1

The other options are not as effective as reconfiguring the web application firewall to block the attack. Force password changes on the SQL database is a reactive measure that does not address the root cause of the problem, and may cause data loss or corruption if not done properly. Updating the detection patterns on the web application firewall is a preventive measure that can help to detect SQL injection attacks, but it does not stop them from happening in the first place. Blocking IPs from where the attack originates is a defensive measure that can limit or stop some SQL injection attacks, but it does not protect all possible sources of malicious traffic, and may also affect legitimate users or applications1

Reference = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 32-33…

Question: 427

Which of the following should an information security manager do FIRST after discovering that a business unit has implemented a newly purchased application and bypassed the change management process?

A. Revise the procurement process.
B. Update the change management process.
C. Discuss the issue with senior leadership.
D. Remove the application from production.

Answer: C

Explanation:

An information security manager should first discuss the issue with senior leadership to escalate the problem and seek their support and guidance. Bypassing the change management process can introduce significant risks to the organization, such as unauthorized access, data loss, system instability, or compliance violations. The information security manager should explain the potential impact and consequences of the incident, and recommend corrective actions to remediate the situation. The information security manager should also review the root cause of the incident and identify any gaps or weaknesses in the existing policies, procedures, or controls that allowed the business unit to implement the new application without proper authorization, testing, or documentation. The information security manager should then revise the procurement process, update the change management process, or implement other measures to prevent similar incidents from occurring in the future. Removing the application from production may not be feasible or desirable, depending on the business needs and the severity of the risks involved. Reference = CISM Review Manual, 16th Edition, pages 100-1011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2692

Learn more:
1. isaca.org2. amazon.com3. gov.uk

Question: 428

The effectiveness of an incident response team will be GREATEST when:

A. the incident response team meets on a regular basis to review log files.
B. the incident response team members are trained security personnel.
C. the incident response process is updated based on lessons learned.
D. incidents are identified using a security information and event monitoring {SIEM) system.

Answer: C

Explanation:

Question: 429

When determining an acceptable risk level which of the following is the MOST important consideration?

A. Threat profiles
B. System criticalities
C. Vulnerability scores
D. Risk matrices

Answer: C

Explanation:

The effectiveness of an incident response team will be greatest when the incident response process is updated based on lessons learned. This ensures that the team can continuously improve its performance and capabilities, and address any gaps or weaknesses identified during previous incidents. Updating the incident response process based on lessons learned also helps to align the process with the changing business and security environment, and to incorporate best practices and standards. Meeting on a regular basis to review log files, having trained security personnel as team members, and using a security information and event monitoring (SIEM) system are all important factors for an incident response team, but they are not sufficient to ensure the effectiveness of the team. Reviewing log files may help to detect and analyze incidents, but it does not guarantee that the team can respond appropriately and efficiently. Having trained security personnel may enhance the skills and knowledge of the team, but it does not ensure that the team can work collaboratively and communicate effectively. Using a SIEM system may facilitate the identification and prioritization of incidents, but it does not ensure that the team can follow the established procedures and protocols. Reference = CISM Review Manual, 16th Edition, page 1361; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492

Question: 430

Which of the following has the GREATEST impact on efforts to improve an organization's security posture?

A. Regular reporting to senior management
B. Supportive tone at the top regarding security
C. Automation of security controls
D. Well-documented security policies and procedures

Answer: B

Explanation:

The supportive tone at the top regarding security is the greatest impact on efforts to improve an organization’s security posture. This means that senior management should demonstrate their commitment and leadership to information security by setting clear goals, allocating adequate resources, communicating effectively, and rewarding good practices. A supportive tone at the top can also influence the culture and behavior of the

organization, as well as foster trust and collaboration among stakeholders12. Reference = CISM Review Manual 15th Edition, page 1261; CISM Item Development Guide, page 82

Question: 431

Which of the following is the MOST effective way to detect security incidents?

A. Analyze recent security risk assessments.
B. Analyze security anomalies.
C. Analyze penetration test results.
D. Analyze vulnerability assessments.

Answer: B

Explanation:

Analyzing security anomalies is the most effective way to detect security incidents, as it involves comparing the current state of the information system and network with the expected or normal state, and identifying any deviations or irregularities that may indicate a security breach or compromise. Security anomalies can be detected by using various tools and techniques, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), log analysis, network traffic analysis, and behavioral analysis. (From CISM Review Manual 15th Edition)

Reference: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; CISM: Information Security Incident Management Part 11, section recognize security anomalies.

Question: 432

Which of the following will BEST enable an effective information asset classification process?

A. Including security requirements in the classification process
B. Analyzing audit findings
C. Reviewing the recovery time objective (RTO) requirements of the asset
D. Assigning ownership

Answer: D

Explanation:

Assigning ownership is the best way to enable an effective information asset classification process, as it establishes the authority and responsibility for the information asset and its protection. The owner of the information asset should be involved in the classification process, as they have the best knowledge of the value, sensitivity, and criticality of the asset, as well as the impact of its loss or compromise. The owner should also ensure that the asset is properly labeled, handled, and secured according to its classification level. (From CISM Review Manual 15th Edition)

Reference: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Information Asset and Security Classification Procedure1, section 3.1.

Question: 433

Which of the following components of an information security risk assessment is MOST valuable to senior management?

A. Threat profile
B. Residual risk
C. Return on investment (ROI)
D. Mitigation actions

Answer: B

Explanation:

Residual risk is the risk that remains after implementing risk mitigation actions. It is the most valuable component for senior management because it helps them to evaluate the effectiveness and efficiency of risk management and make informed decisions about risk acceptance, transfer or avoidance. Reference = CISM Review Manual, 16th Edition, Chapter 2, Section 2.3.41

Question: 434

Application data integrity risk is MOST directly addressed by a design that includes:

A. reconciliation routines such as checksums, hash totals, and record counts.
B. strict application of an authorized data dictionary.
C. application log requirements such as field-level audit trails and user activity logs.
D. access control technologies such as role-based entitlements.

Answer: A

Explanation:

Reconciliation routines are methods to verify the integrity of data by comparing the input and output of a process or a system. They can detect errors, omissions, duplications or unauthorized modifications of data. They are more directly related to data integrity than the other options, which are more concerned with data definition, logging or access control. Reference = CISM Review Manual, 16th Edition, Chapter 3, Section 3.4.21

Question: 435

When drafting the corporate privacy statement for a public website, which of the following MUST be included?

A. Limited liability clause
B. Explanation of information usage

C. Information encryption requirements
D. Access control requirements

Answer: B

Explanation:

A privacy statement should inform the users of the website how their personal information will be collected, used, shared, and protected by the organization. Reference = CISM Review Manual, 16th Edition, Chapter 4, Section 4.2.1.11

Question: 436

For which of the following is it MOST important that system administrators be restricted to read-only access?

A. User access log files
B. Administrator user profiles
C. Administrator log files
D. System logging options

Answer: A

Explanation:

User access log files contain records of user activities and actions on the system, which can be used for auditing, monitoring, and investigating purposes. System administrators should not be able to modify or delete these files to ensure their integrity and availability. Reference = CISM Review Manual, 16th Edition, Chapter 3, Section 3.3.2.11

Question: 437

Which of the following BEST enables an organization to maintain an appropriate security control environment?

A. Alignment to an industry security framework
B. Budgetary support for security
C. Periodic employee security training
D. Monitoring of the threat landscape

Answer: A

Explanation:

Alignment to an industry security framework ensures that the organization adopts best practices and standards for security control implementation and maintenance. Reference = CISM Review Manual, 16th Edition, Domain

1: Information Security Governance, Chapter 1: Establish and Maintain an Information Security Strategy, Section: Information Security Frameworks

Question: 438

Who is accountable for approving an information security governance framework?

A. The board of directors
B. The chief information security officer (CISO)
C. The enterprise risk committee
D. The chief information officer (CIO)

Answer: A

Explanation:

The board of directors is ultimately responsible for the governance of the organization, including the approval of the information security governance framework and the oversight of its implementation and performance. Reference = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 2: Establish and Maintain an Information Security Governance Framework,

Section: Roles and Responsibilities of Senior Management and the Board of Directors1

Question: 439

Which of the following is the PRIMARY benefit achieved when an information security governance framework is aligned with corporate governance?

A. Protection of business value and assets
B. Identification of core business strategiesC, Easier entrance into new businesses and technologies
C. Improved regulatory compliance posture

Answer: A

Explanation:

Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed. By aligning information security governance with corporate governance, the organization can ensure that information security is integrated into the business processes and decision making, and that the information security risks and opportunities are properly identified, assessed, and addressed. Reference = CISM Review Manual, 16th Edition, Chapter 1, Section 1.1

Question: 440

The GREATEST challenge when attempting data recovery of a specific file during forensic analysis is when:

A. the partition table on the disk has been deleted.
B. the tile has been overwritten.
C. all files in the directory have been deleted.
D. high-level disk formatting has been performed.

Answer: B

Explanation:

Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system. Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data. However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table, the directory, and the formatting information can be reconstructed or bypassed by using forensic tools. Reference = CISM Review Manual, 16th Edition, Chapter 5, Section

5.4.1.2

Question: 441

An information security manager wants to document requirements detailing the minimum security controls required for user workstations. Which of the following resources would be MOST appropriate for this purposed?

A. Guidelines
B. Policies
C. Procedures
D. Standards

Answer: D

Explanation:

Standards are detailed statements of the minimum requirements for hardware, software, or security configurations. They are used to define the minimum security controls required for user workstations. Reference = CISM Review Manual, 16th Edition, page 69.

Question: 442

Which of the following is the BEST method to protect the confidentiality of data transmitted over the Internet?

A. Network address translation (NAT)

B. Message hashing
C. Transport Layer Security (TLS)
D. Multi-factor authentication

Answer: C

Explanation:

Transport Layer Security (TLS) is a protocol that provides encryption, authentication, and integrity for data transmitted over the Internet. TLS protects the confidentiality of data by encrypting it before sending it and decrypting it after receiving it. TLS also verifies the identity of the communicating parties by using certificates and prevents data tampering by using message authentication codes. Reference = CISM Review Manual, 16th Edition, Chapter 4, Section 4.3.2.11

Question: 443

Which of the following is the FIRST step when conducting a post-incident review?

A. Identify mitigating controls.
B. Assess the costs of the incident.
C. Perform root cause analysis.
D. Assign responsibility for corrective actions.

Answer: C

Explanation:

A post-incident review is a process of analyzing an incident and its impact, identifying the root causes, and recommending corrective actions to prevent recurrence. The first step of a post-incident review is to perform root cause analysis, which is the process of identifying the underlying factors that contributed to the occurrence and severity of the incident. Root cause analysis helps to determine the most effective and efficient solutions to address the problem and avoid future incidents. Reference = CISM Review Manual, 16th Edition, Chapter 5, Section 5.5.2.11

Question: 444

Which of the following BEST facilitates the effectiveness of cybersecurity incident response?

A. Utilizing a security information and event management (SIEM) tool.
B. Utilizing industry-leading network penetration testing tools.
C. Increasing communication with all incident response stakeholders.
D. Continuously updating signatures of the anti-malware solution.

Answer: C

Explanation:

Communication is a key factor for the effectiveness of cybersecurity incident response, as it ensures that all relevant parties are informed, coordinated, and aligned on the incident status, impact, actions, and responsibilities. Communication also helps to maintain trust, confidence, and transparency among the stakeholders, such as senior management, business units, customers, regulators, law enforcement, and media. Reference = CISM Review Manual, 16th Edition, Chapter 5, Section 5.4.2.11

Question: 445

Which of the following is the MOST important constraint to be considered when developing an information security strategy?

A. Legal and regulatory requirements
B. Established security policies and standards
C. Compliance with an international security standard
D. Information security architecture

Answer: A

Explanation:

Legal and regulatory requirements are the most important constraint to be considered when developing an information security strategy, as they define the minimum level of security that the organization must comply with to avoid legal sanctions, fines, or reputational damage. Legal and regulatory requirements may vary depending on the jurisdiction, industry, and type of data that the organization handles, and they may impose specific security controls, standards, or frameworks that the organization must follow. Reference = CISM Review Manual, 16th Edition, Chapter 1, Section 1.2.1.11

Question: 446

An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done NEXT to address this concern?

A. Escalate to the chief risk officer (CRO).
B. Conduct a vulnerability analysis.
C. Conduct a risk analysis.
D. Determine compensating controls.

Answer: C

Explanation:

A risk analysis is the next step to identify and evaluate the potential security risks associated with a third-party service provider and determine the appropriate risk response strategies. Reference = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 1231241

Question: 447

What is the role of the information security manager in finalizing contract negotiations with service providers?

A. To perform a risk analysis on the outsourcing process
B. To obtain a security standard certification from the provider
C. To update security standards for the outsourced process
D. To ensure that clauses for periodic audits are included

Answer: A

Explanation:

The role of the information security manager in finalizing contract negotiations with service providers is to ensure that the outsourcing process is aligned with the organization's information security policies, standards, and objectives. One of the key aspects of this process is to perform a risk analysis on the outsourcing process, which involves identifying, assessing, and mitigating the potential threats and vulnerabilities that may arise from outsourcing activities. A risk analysis can help the information security manager to determine the appropriate level of security controls and requirements for the outsourced process, as well as to monitor and evaluate its performance and compliance. A risk analysis can also help to avoid or minimize legal, financial, reputational, or operational risks associated with outsourcing1. Reference =
CISM Review Manual (Digital Version), Chapter 6: Information Security Program Management
CISM Review Manual (Print Version), Chapter 6: Information Security Program Management

Question: 448

Recommendations for enterprise investment in security technology should be PRIMARILY based on:

A. adherence to international standards
B. availability of financial resources
C. the organization s risk tolerance
D. alignment with business needs

Answer: C

Explanation:

Verified Answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section Explanation:3.2.1.1, "Recommendations for enterprise investment in security technology should be primarily based on the organization's risk tolerance."1
Comprehensive and Detailed The organization's risk tolerance is the degree of uncertainty that the organization is willing to accept in order to pursue its objectives. It reflects the organization's appetite for risk and its ability to cope with potential losses or disruptions. The higher the risk tolerance, the more aggressive and innovative the security investments can be, as they can help achieve faster growth or competitive advantage. The lower the risk tolerance, the more conservative and defensive the security investments should

be, as they can help protect the organization's assets and reputation from potential threats.

Reference: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1

Question: 449

A business impact analysis (BIA) should be periodically executed PRIMARILY to:

A. validate vulnerabilities on environmental changes.
B. analyze the importance of assets.
C. check compliance with regulations.
D. verify the effectiveness of controls.

Answer: D

Explanation:

A business impact analysis (BIA) is a process that helps identify and evaluate the potential effects of disruptions or incidents on the organization's mission, objectives, and operations. A BIA should be periodically executed to verify the effectiveness of the controls that are implemented to prevent, mitigate, or recover from such disruptions or incidents12.

According to the CISM Manual, a BIA should be performed at least annually for critical systems and processes, and more frequently for non-critical ones3. A BIA should also be updated whenever there are significant changes in the organization's environment, such as new regulations, technologies, business models, or stakeholder expectations3. A BIA should not be used to validate vulnerabilities on environmental changes (A), analyze the importance of assets (B), or check compliance with regulations ©, as these are not the primary purposes of a BIA.

Reference: 1: IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response | CSRC NIST 2: CISM Domain 4 Preview | BCP - Business Impact Analysis (BIA) - YouTube 3: CISM ITEM DEVELOPMENT GUIDE - ISACA

Question: 450

Which of the following roles is PRIMARILY responsible for developing an information classification framework based on business needs?

A. Information security manager
B. Information security steering committee
C. Information owner
D. Senior management

Answer: C

Explanation:

According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, Information owners are responsible for developing an information classification framework based on business needs1. They are also responsible for defining and maintaining the classification scheme, policies, and procedures for their information assets1.

The CISM Review Manual (Digital Version) also states that information owners should collaborate with other stakeholders, such as information security managers, information security steering committees, senior management, and legal counsel, to ensure that the classification framework is aligned with the organization's objectives and complies with applicable laws and regulations1.

The CISM Exam Content Outline also covers the topic of information classification frameworks in Domain 3 — Information Security Program Development and Management (27% exam weight)2. The subtopics include:

3.2.1 Information Classification Frameworks
3.2.2 Information Classification Policies
3.2.3 Information Classification Procedures
3.2.4 Information Classification Training

I hope this answer helps you prepare for your CISM exam. Good luck!

Question: 451

During the implementation of a new system, which of the following processes proactively minimizes the likelihood of disruption, unauthorized alterations, and errors?

A. Configuration management
B. Password management
C. Change management
D. Version management

Answer: C

Explanation:

Change management is the process of planning, implementing, and monitoring changes to information systems in a controlled and coordinated manner. Change management proactively minimizes the likelihood of disruption, unauthorized alterations, and errors by ensuring that changes are aligned with the organization's objectives, policies, and procedures. Change management also involves identifying and mitigating the risks associated with changes, as well as communicating and documenting the changes to all relevant stakeholders12.

Reference = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

Question: 452

Which of the following factors would have the MOST significant impact on an organization's information security governance mode?

A. Outsourced processes
B. Security budget
C. Number of employees
D. Corporate culture

Answer: D

Explanation:

The corporate culture of an organization is the set of values, beliefs, norms, and behaviors that shape how the organization operates and interacts with its stakeholders. The corporate culture can have a significant impact on an organization's information security governance mode, which is the way the organization establishes, implements, monitors, and evaluates its information security policies, standards, and objectives. A strong information security governance mode requires a supportive corporate culture that fosters a shared vision, commitment, and accountability for information security among all levels of the organization. A supportive corporate culture can also help to overcome resistance to change, promote collaboration and communication, encourage innovation and learning, and enhance trust and confidence in information security12. Reference = CISM Review Manual (Digital Version), Chapter 1: Information Security Governance CISM Review Manual (Print Version), Chapter 1: Information Security Governance

Question: 453

Embedding security responsibilities into job descriptions is important PRIMARILY because it:

A. supports access management.
B. simplifies development of the security awareness program.
C. aligns security to the human resources (HR) function.
D. strengthens employee accountability.

Answer: D

Explanation:

Comprehensive and Detailed Employee accountability is the degree to which employees are responsible for their actions and outcomes related to information security. It reflects the extent to which employees understand their roles and responsibilities, follow the policies and procedures, report incidents and breaches, and comply with legal and regulatory requirements. Embedding security responsibilities into job descriptions helps to clarify the expectations and obligations of employees, as well as the consequences of non-compliance or negligence. It also helps to align the security objectives with the business goals and strategies, and to foster a culture of security awareness and responsibility.
Reference: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.2

Question: 454

Which of the following is the MOST important consideration when updating procedures for managing

security devices?

A. Updates based on the organization's security framework
B. Notification to management of the procedural changes
C. Updates based on changes m risk technology and process
D. Review and approval of procedures by management

Answer: C

Explanation:

According to the CISM Manual, updating procedures for managing security devices should be based on changes in risk technology and process, not on the organization's security framework, notification to management of the procedural changes, or review and approval of procedures by management1. These are not the most important considerations when updating procedures for managing security devices, as they do not reflect the actual impact of the changes on the security posture of the organization.

The CISM Manual states that "procedures for managing security devices should be updated whenever there are significant changes in the risk technology or process that affect the security devices" (IR 8287A)1. For example, if a new security device is introduced or an existing one is replaced, its procedures should be updated accordingly. Similarly, if a new risk technology or process is implemented that affects how security devices are configured, monitored, or maintained, its procedures should be updated as well1.

The CISM Manual also provides guidance on how to update procedures for managing security devices in a systematic and consistent manner. It recommends using a change management process that involves identifying, analyzing, approving, implementing, and evaluating changes to security device procedures1. It also suggests using a change control board (CCB) that consists of representatives from different stakeholders who review and approve changes to security device procedures before they are implemented1.

Reference: 1: IR 8287A - Managing Security Devices | CSRC NIST

Question: 455

When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?

A. Configuration management
B. Risk management
C. Access control management
D. Change management

Answer: D

Explanation:

According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.2, change management is the process of identifying, assessing, approving, implementing, and monitoring changes to information systems and information security controls1. Change management is essential for ensuring that changes are aligned with the

organization's business strategy and objectives, as well as complying with applicable laws and regulations1.

The CISM Review Manual (Digital Version) also states that change management should be performed in conjunction with other processes, such as configuration management, access control management, and risk management1. Configuration management is the process of identifying, documenting, controlling, and verifying the configuration items (CIs) of an information

system1. Access control management is the process of granting or denying access to information systems and information assets based on predefined policies and procedures1. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks to information systems and information assets1.

The CISM Exam Content Outline also covers the topic of change management in Domain 3 — Information Security Program Development and Management (27% exam weight)2. The subtopics include:

3.2.2 Change Management

3.2.3 Change Control

3.2.4 Change Implementation

3.2.5 Change Monitoring

I hope this answer helps you prepare for your CISM exam. Good luck!

Question: 456

An information security manager learns that business unit leaders are encouraging increased use of social media platforms to reach customers. Which of the following should be done FIRST to help mitigate the risk of confidential information being disclosed by employees on social media?

A. Establish an organization-wide social media policy.
B. Develop sanctions for misuse of social media sites.
C. Monitor social media sites visited by employees.
D. Restrict social media access on corporate devices.

Answer: A

Explanation:

An organization-wide social media policy is a document that defines the rules and guidelines for using social media platforms within the organization. It covers topics such as who can use social media, what they can post, how they should protect confidential information, and what are the consequences for violating the policy. An organization-wide social media policy helps to mitigate the risk of confidential information being disclosed by employees on social media by providing a clear and consistent framework for managing social media activities12.

Reference = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

Question: 457

A technical vulnerability assessment on a personnel information management server should be performed

when:

A. the data owner leaves the organization unexpectedly.
B. changes are made to the system configuration.
C. the number of unauthorized access attempts increases.
D. an unexpected server outage has occurred.

Answer: B

Explanation:

A technical vulnerability assessment is a process of identifying and evaluating the weaknesses and risks associated with a specific system, component, or network. A technical vulnerability assessment can help to determine the potential impact and likelihood of a security breach, as well as the appropriate measures to prevent or mitigate it. A technical vulnerability assessment should be performed on a personnel information management server whenever there is an increase in the number of unauthorized access attempts to the server, as this indicates that the server may have been compromised or targeted by an attacker12. Therefore, option C is the correct answer. Reference =
CISM Review Manual (Digital Version), Chapter 5: Information Security Program Management
CISM Review Manual (Print Version), Chapter 5: Information Security Program Management

Question: 458

A recent application security assessment identified a number of low- and medium-level vulnerabilities. Which of the following stakeholders is responsible for deciding the appropriate risk treatment option?

A. Security manager
B. Chief information security officer (CISO)
C. System administrator
D. Business owner

Answer: B

Explanation:

Verified Answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section Explanation:3.2.1.3, "The appropriate risk treatment option is decided by the chief information security officer (CISO) or the designated risk owner."1
Comprehensive and Detailed The CISO is the senior executive who is responsible for overseeing and managing the information security program of an organization. The CISO has the authority and expertise to assess the risks, determine the risk appetite and tolerance levels, and select the most suitable risk treatment options for each risk. The CISO also has the accountability and responsibility for implementing, monitoring, and reporting on the risk treatment activities.
Reference: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3

Question: 459

Which of the following would BEST guide the development and maintenance of an information security program?

A. A business impact assessment
B. A comprehensive risk register
C. An established risk assessment process
D. The organization's risk appetite

Answer: D

Explanation:

According to the CISM Manual, the organization's risk appetite is the amount and type of risk that the organization is willing to accept in order to achieve its objectives1. The organization's risk appetite should guide the development and maintenance of an information security program, as it determines the level of security controls, resources, and activities that are needed to protect the organization's assets and operations1.
The CISM Manual states that "the information security program should be aligned with the organization's risk appetite, which reflects its tolerance for risk and its strategic objectives" (IR 8288A)1. The information security program should also consider other factors that influence the organization's risk appetite, such as its mission, vision, values, culture, stakeholders, regulations, standards, guidelines, and best practices1.
The CISM Manual also provides guidance on how to develop and maintain an information security program based on the organization's risk appetite. It recommends using a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that affect the organization's information assets1. It also suggests using a framework or model that supports the development of an information security program based on the organization's risk appetite (e.g., ISO/IEC 27001)1.
Reference: 1: IR 8288A - Information Security Program Development | CSRC NIST

Question: 460

Which of the following should be the PRIMARY outcome of an information security program?

A. Strategic alignment
B. Risk elimination
C. Cost reduction
D. Threat reduction

Answer: A

Explanation:

According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, strategic alignment is the primary outcome of an information security program1. Strategic alignment means that the information security program supports and is tailored to the organization's objectives and business strategy1. It also means that the information security program is aligned with other assurance

functions, such as physical, human resources, quality, and IT1.
The CISM Review Manual (Digital Version) also states that strategic alignment is essential for achieving a competitive advantage, enhancing customer trust, reducing legal and regulatory risks, and improving organizational performance1. Strategic alignment requires effective communication and collaboration among all stakeholders, including senior management, information owners, information security managers, information security steering committees, and external partners1. The CISM Exam Content Outline also covers the topic of strategic alignment in Domain 3 — Information Security Program Development and Management (33% exam weight)2. The subtopics include:

3.2.1 Information Security Strategy
3.2.2 Information Security Governance
3.2.3 Information Security Risk Management
3.2.4 Information Security Compliance

I hope this answer helps you prepare for your CISM exam. Good luck!

Question: 461

A new regulatory requirement affecting an organization's information security program is released. Which of the following should be the information security manager's FIRST course of action?

A. Perform a gap analysis.
B. Conduct benchmarking.
C. Notify the legal department.
D. Determine the disruption to the business.

Answer: C

Explanation:

= A new regulatory requirement affecting an organization's information security program is released. The information security manager's first course of action should be to notify the legal department, as they are responsible for ensuring compliance with the relevant laws and regulations. The legal department can advise the information security manager on how to interpret and implement the new requirement, as well as what are the potential implications and risks for the organization12.

Reference = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

Learn more:

1. isaca.org2. csoonline.com

Question: 462

Which of the following is MOST important to maintain integration among the incident response plan, business continuity plan (BCP). and disaster recovery plan (DRP)?

A. Asset classification
B. Recovery time objectives (RTOs)
C. Chain of custody
D. Escalation procedures

Answer: B

Explanation:

Recovery time objectives (RTOs) are the maximum acceptable time that an organization can be ofline or unavailable after a disruption. RTOs are important to maintain integration among the incident response plan, business continuity plan (BCP), and disaster recovery plan (DRP) because they help align the recovery goals and strategies of each plan. By defining clear and realistic RTOs, an organization can ensure that its IT infrastructure and systems are restored as quickly as possible after a disaster, minimizing the impact on business operations and customer satisfaction.

Reference = CISM Manual, Chapter 6: Incident Response Planning, Section 6.2: Recovery Time Objectives (RTOs), page 971

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

Question: 463

Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?

A. Perform a vulnerability assessment
B. Perform a gap analysis to determine needed resources
C. Create a security exception
D. Assess the risk to business operations

Answer: D

Explanation:

According to the CISM Manual, the information security manager should first assess the risk to business operations before taking any other action. This will help to prioritize the issues and determine the appropriate response. Performing a vulnerability assessment, a gap analysis, or creating a security exception are possible actions, but they should be based on the risk assessment results. Reference = CISM Manual, 5th Edition, page 1211; CISM Practice Quiz, question 32

Question: 464

An information security program is BEST positioned for success when it is closely aligned with:

A. information security best practices.
B. recognized industry frameworks.
C. information security policies.
D. the information security strategy.

Answer: D

Explanation:

An information security program is best positioned for success when it is closely aligned with the information security strategy, which defines the organization's vision, mission, goals, objectives, and risk appetite for information security. The information security strategy provides the direction and guidance for developing and implementing the information security program, ensuring that it supports the organization's business processes and objectives. The information security strategy also helps to establish the scope, boundaries, roles, responsibilities, and resources for the information security program.
Reference = CISM Manual, Chapter 3: Information Security Program Development (ISPD), Section 3.1: Information Security Strategy1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

Question: 465

Which of the following should be established FIRST when implementing an information security governance framework?

A. Security architecture
B. Security policies
C. Security incident management team
D. Security awareness training program

Answer: A

Explanation:

This is the most urgent and effective action to prevent further damage or compromise of the organization's network and data. The other options are less important or irrelevant in this situation. According to How to identify suspicious insider activity using Active Directory, one of the steps to detect and respond to suspicious activity is to isolate the affected device from the network. This can be done by disabling the network adapter, unplugging the network cable, or blocking the device's IP address on the firewall1. This will prevent the device from communicating with any malicious actors or spreading malware to other devices on the network.

Question: 466

Which of the following should an information security manager do FIRST after identifying suspicious activity on a PC that is not in the organization's IT asset inventory?

A. Isolate the PC from the network
B. Perform a vulnerability scan
C. Determine why the PC is not included in the inventory
D. Reinforce information security training

Answer: C

Explanation:

The first thing an information security manager should do after identifying suspicious activity on a PC that is not in the organization's IT asset inventory is to determine why the PC is not included in the inventory. This will help to identify the source and scope of the threat, as well as the potential impact and risk to the organization. The IT asset inventory is a list of all the hardware, software, data, and other resources that are owned, controlled, or used by an organization. It helps to establish accountability, visibility, and control over the IT assets, as well as to support security policies and procedures.

If a PC is not included in the inventory, it may indicate that it has been compromised by an unauthorized user or entity, or that it has been moved or transferred without proper authorization. It may also indicate that there are gaps or errors in the inventory management process, such as missing records, duplicate entries, outdated information, or inaccurate classification. These issues can pose significant challenges for information security management, such as:

Lack of visibility into the IT environment and assets

Difficulty in detecting and responding to incidents

Increased risk of data breaches and cyberattacks

Non-compliance with regulatory requirements and standards

Reduced trust and confidence among stakeholders

Therefore, an information security manager should take immediate steps to investigate why the PC is not included in the inventory and take appropriate actions to remediate the situation.

Reference = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Inventory Management1

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

Question: 467

An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

A. File integrity monitoring software
B. Security information and event management (SIEM) tool
C. Antivirus software
D. Intrusion detection system (IDS)

Answer: D

Explanation:

An intrusion detection system (IDS) is a software or hardware device that monitors network traffic and detects unauthorized or malicious activities, such as attacks, intrusions, or breaches. An IDS can provide valuable evidence for an information security team to investigate an alleged breach of an organization's network, as it can capture and analyze the network traffic in real time or after the fact. An IDS can help to identify the source, type, scope, and impact of the breach, as well as to generate alerts and reports for further investigation.

File integrity monitoring software (FIM), security information and event management (SIEM) tool, and antivirus software are not single sources of evidence for an information security team to review. FIM software monitors

files and directories on a network or system and detects changes or modifications that may indicate unauthorized access or tampering. SIEM tool collects and correlates data from various sources, such as logs, events, alerts, incidents, and threats, and provides a unified view of the security posture of an organization. Antivirus software scans files and programs on a network or system and detects malware infections that may compromise the security or functionality of the system.

However, these tools are not sufficient by themselves to provide conclusive evidence for an information security team to investigate an alleged breach of an organization's network. They may provide some clues or indicators of compromise (IOCs), but they may also generate false positives or negatives due to various factors, such as configuration errors, user behavior, benign activities, or evasion techniques. Therefore, an information security team should use multiple sources of evidence from different tools and methods to verify the validity and reliability of the findings.

Reference = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Evidence Collection1 1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

Question: 468

Which of the following should an organization do FIRST when confronted with the transfer of personal data across borders?

A. Define policies and standards for data processing.
B. Implement applicable privacy principles
C. Assess local or regional regulations
D. Research cyber insurance policies

Answer: C

Explanation:

Before transferring personal data across borders, an organization should first assess the local or regional regulations that apply to the data protection and privacy of the data subjects. This will help the organization to identify the legal requirements and risks involved in the data transfer, and to choose the appropriate tools and safeguards to ensure compliance and protection. For example, the organization may need to obtain consent from the data subjects, use adequacy decisions, standard contractual clauses, or other mechanisms to ensure an adequate level of protection in the third country, or rely on specific derogations for certain situations. The other options are not the first steps

to take, although they may be relevant at later stages of the data transfer process. Reference = Guide to the cross-border transfer of personal data in the GDPR
New guidance issued by the EDPB on international transfers of personal data
Requirements for transferring personal information across borders

Question: 469

During which of the following development phases is it MOST challenging to implement security controls?

A. Post-implementation phase

B. Implementation phase

C. Development phase

D. Design phase

Answer: C

Explanation:

The development phase is the stage of the system development life cycle (SDLC) where the system requirements, design, architecture, and implementation are performed. The development phase is most challenging to implement security controls because it involves complex and dynamic processes that may not be well understood or documented. Security controls are essential for ensuring the confidentiality, integrity, and availability of the system and its data, as well as for complying with regulatory and contractual obligations. However, security controls may also introduce additional costs, risks, and constraints to the development process, such as:

Increased complexity and overhead of testing, verification, validation, and maintenance Reduced flexibility and agility of changing requirements or design

Increased dependency on external vendors or third parties for security services or products Increased vulnerability to errors, defects, or vulnerabilities in the code or configuration Increased difficulty in measuring and reporting on security performance or effectiveness Therefore, implementing security controls in the development phase requires careful planning, coordination, communication, and collaboration among all stakeholders involved in the SDLC. It also requires a clear understanding of the security objectives, scope, criteria, standards, policies, procedures, roles, responsibilities, and resources for the system. Moreover, it requires a proactive approach to identifying and mitigating potential threats or risks that may affect the security of the system.

Reference = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1: System Development Life Cycle (SDLC)2

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

Question: 470

Which of the following is the MOST important consideration when briefing executives about the current state of the information security program?

A. Including a situational forecast

B. Using appropriate language for the target audience

C. Including trend charts for metrics

D. Using a rating system to demonstrate program effectiveness

Answer: D

Explanation:

= When briefing executives about the current state of the information security program, the most important consideration is to use appropriate language for the target audience. This means avoiding technical jargon,

acronyms, and details that may confuse or bore the executives, and instead focusing on the business value, risks, and benefits of the information security program. The other options are not as important or relevant as using appropriate language, although they may also be useful to include in the briefing. For example, a situational forecast may be helpful to show the future trends and challenges, but it is not as essential as communicating the current state clearly and concisely. Similarly, trend charts for metrics and a rating system to demonstrate program effectiveness may be useful to support the briefing, but they are not as critical as using language that the executives can understand and relate to. Reference =
Information Security Guide for Government Executives, page 7: "Reminding employees of their responsibilities and demonstrating management's commitment to the security program are key to maintaining effective security within the constantly changing information security environment." Information security guide for government executives - NIST, page 3: "The executive should communicate the importance of information security to the organization and its staff, using language that is meaningful to the target audience." Information Security Committee Charter - SecurityStudio, page 1: "The committee also coordinates and communicates the direction, current state, and oversight of the information security program."

Question: 471

Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

A. a function of the likelihood and impact, should a threat exploit a vulnerability.
B. the magnitude of the impact, should a threat exploit a vulnerability.
C. a function of the cost and effectiveness of controls over a vulnerability.
D. the likelihood of a given threat attempting to exploit a vulnerability

Answer: A

Explanation:

= According to the CISM Manual1, risk is defined as the combination of the probability of an event and its consequence. Therefore, determining the risk for a particular threat/vulnerability pair before

controls are applied can be expressed as a function of the likelihood and impact, should a threat exploit a vulnerability. Likelihood is the probability or frequency of a threat occurring, while impact is the magnitude or severity of the harm or loss that would result from a threat exploiting a vulnerability. The higher the likelihood and impact, the higher the risk. The lower the likelihood and impact, the lower the risk.
The other options are not correct because they do not capture the full expression of risk. Option B only considers the impact, but not the likelihood, of a threat exploiting a vulnerability. Option C confuses the risk with the risk response, which is the action taken to reduce or mitigate the risk. Option D only considers the likelihood, but not the impact, of a threat attempting to exploit a vulnerability.
Reference = CISM Manual1, Chapter 2: Information Risk Management (IRM), Section 2.1: Risk Concepts2 1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 2

Question: 472

Which of the following defines the MOST comprehensive set of security requirements for a newly developed

information system?

A. Risk assessment results
B. Audit findings
C. Key risk indicators (KRIs)
D. Baseline controls

Answer: D

Explanation:

Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance. Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security requirements, or they may vary depending on the system or the context. For example, risk assessment results are an important input for defining the security requirements, but they are not the requirements themselves. Audit findings are an output of evaluating the compliance and effectiveness of the security requirements, but they are not the requirements themselves. Key risk indicators (KRIs) are metrics that measure the level of risk exposure and performance of the security requirements, but they are not the requirements themselves. Reference =
CISM Review Manual 15th Edition, page 113: "Baseline controls are the minimum security requirements that apply to all systems within the organization."
CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question 478: "Baseline controls are the minimum security requirements that apply to all systems within the organization. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance."

Question: 473

Which of the following is ESSENTIAL to ensuring effective incident response?

A. Business continuity plan (BCP)
B. Cost-benefit analysis
C. Classification scheme
D. Senior management support

Answer: D

Explanation:

Senior management support is essential to ensuring effective incident response because it provides the necessary authority, resources, and guidance for the information security team to perform their roles and responsibilities. Senior management support also helps to establish the goals, scope, policies, and procedures

for the incident response plan (IRP), as well as to ensure its alignment with the business objectives and strategy. Senior management support also fosters a culture of security awareness, accountability, and collaboration among all stakeholders involved in the incident response process.

The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality.

Reference = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1: Incident Response Plan2

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 4

Question: 474

Which of the following is the BEST approach for data owners to use when defining access privileges for users?

Define access privileges based on user roles.

Adopt user account settings recommended by the vendor.

Perform a risk assessment of the users' access privileges.

A. Implement an identity and access management (IDM) tool.

Answer: A

Explanation:

This approach is the best because it ensures that users have the minimum level of access required to perform their job functions, which reduces the risk of unauthorized access or misuse of data. User roles are defined based on the business needs and responsibilities of the users, and they can be easily managed and audited.

Reference: The CISM Review Manual 2023 states that “the data owner is responsible for defining the access privileges for each user role” and that “the data owner should ensure that the principle of least privilege is applied to all users” (p. 82). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: “Defining access privileges based on user roles is the best approach because it allows the data owner to assign the minimum level of access required for each role and to review and update the roles periodically” (p. 23).

Question: 475

Following an employee security awareness training program, what should be the expected outcome?

A. A decrease in the number of viruses detected in incoming emails
B. A decrease in reported social engineering attacks
C. An increase in reported social engineering attempts
D. An increase in user-reported false positive incidents

Answer: C

Explanation:

This outcome indicates that the employees are more aware of the signs and techniques of social engineering and are able to report them to the appropriate authorities. This also helps to prevent successful attacks and reduce the impact of potential breaches.

Reference: The CISM Review Manual 2023 states that "security awareness training should include information on how to identify and report social engineering attempts" and that "the effectiveness of security awareness training can be measured by the number and quality of reported incidents" (p. 121). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "An increase in reported social engineering attempts is the best indicator that the security awareness training program has been effective, as it shows that the employees are more vigilant and proactive in detecting and reporting such attempts" (p. 45).

Question: 476

An organization has acquired a new system with strict maintenance instructions and schedules. Where should this information be documented?

A. Standards
B. Policies
C. Guidelines
D. Procedures

Answer: D

Explanation:

Procedures are the detailed steps or instructions for performing specific tasks or activities. They are usually aligned with standards, policies and guidelines, but they are more specific and prescriptive. System maintenance instructions and schedules are examples of procedures that should be documented and followed to ensure the proper functioning and security of the system.

Reference: The CISM Review Manual 2023 defines procedures as "the lowest level in the hierarchy of documentation. They are detailed steps that a user must follow to accomplish an activity" (p. 80).

The CISM Item Development Guide also provides the following explanation for this answer: "Procedures are the correct answer because they provide the specific steps to be followed to maintain the system" (p. 11).

Question: 477

Which of the following is the BEST way to enhance training for incident response teams?

A. Perform post-incident reviews.
B. Establish incident key performance indicators (KPIs).
C. Conduct interviews with organizational units.
D. Participate in emergency response activities.

Answer: A

Explanation:

Performing post-incident reviews is the best way to enhance training for incident response teams because it allows them to identify the strengths and weaknesses of their response, learn from the lessons and best practices, and implement corrective actions and improvement plans for future incidents. Post-incident reviews also help to evaluate the effectiveness and efficiency of the incident response process and procedures, and to update them as needed.

Reference: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).

The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Performing post-incident reviews is the best way to enhance

training for incident response teams, as it enables them to learn from their experience and improve their skills and knowledge" (p. 97).

Question: 478

Which of the following should be the PRIMARY focus of a lessons learned exercise following a successful response to a cybersecurity incident?

A. Establishing the root cause of the incident
B. Identifying attack vectors utilized in the incident
C. When business operations were restored after the incident
D. How incident management processes were executed

Answer: D

Explanation:

The primary focus of a lessons learned exercise following a successful response to a cybersecurity incident is to evaluate how the incident management processes were executed, and to identify the strengths, weaknesses,

best practices, and improvement opportunities for future incidents. A lessons learned exercise is not meant to determine the root cause, the attack vectors, or the recovery time of the incident, but rather to assess the performance and effectiveness of the incident response team and the incident response plan.
Reference: The CISM Review Manual 2023 states that “post-incident reviews are an essential part of the incident response process” and that “they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices” (p. 191).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: “How incident management processes were executed is the correct answer because it is the primary focus of a lessons learned exercise, which aims to evaluate the incident response capability and to implement corrective actions and improvement plans” (p. 97). Additionally, the Cybersecurity Incident Response Exercise Guidance article from the ISACA Journal 2022 states that “The AAR [after-action review] should include the date and time of the exercise, a list of participants, scenario descriptions, findings (generic and specific), observations with recommendations, lessons learned and an evaluation of the exercise (strengths, weaknesses, lessons learned)” (p. 3)1

Question: 479

Which of the following should an information security manager do FIRST upon confirming a privileged user's unauthorized modifications to a security application?

A. Report the risk associated with the policy breach.
B. Enforce the security configuration and require the change to be reverted.
C. Implement compensating controls to address the risk.
D. Implement a privileged access management system.

Answer: B

Explanation:

The first thing that an information security manager should do upon confirming a privileged user’s unauthorized modifications to a security application is to enforce the security configuration and require the change to be reverted. This is because the unauthorized modification may have compromised the security of the application and the data it protects, and may have violated the security policies and standards of the organization. By enforcing the security configuration and requiring the change to be reverted, the information security manager can restore the security posture of the application and prevent further unauthorized modifications.
Reference: The CISM Review Manual 2023 states that “the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization” and that “the information security manager should monitor and review the security configuration of information systems on a regular basis and take corrective actions when deviations or violations are detected” (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: “Enforcing the security configuration and requiring the change to be reverted is the correct answer because it is the most immediate and effective action to address the unauthorized modification and to maintain the security of the application” (p. 63). Additionally, the Effective

Interactive Privileged Access Review article from the ISACA Journal 2018 states that "any unauthorized changes to the production environment should be reverted back to the original state and the incident should be reported to the appropriate authority" (p. 4)1.

Question: 480

Which of the following is the MOST important outcome of effective risk treatment?

A. Elimination of risk
B. Timely reporting of incidents
C. Reduced cost of acquiring controls
D. Implementation of corrective actions

Answer: D

Explanation:

The most important outcome of effective risk treatment is the implementation of corrective actions that address the root causes of the risk and reduce its likelihood and/or impact to an acceptable

level. Effective risk treatment does not necessarily eliminate the risk, but rather brings it within the organization's risk appetite and tolerance. Timely reporting of incidents and reduced cost of acquiring controls are desirable benefits of effective risk treatment, but they are not the primary outcome.
Reference: The CISM Review Manual 2023 defines risk treatment as "the process of selecting and implementing measures to modify risk" and states that "the objective of risk treatment is to implement corrective actions that will reduce the risk to a level that is acceptable to the enterprise" (p. 92). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Implementation of corrective actions is the correct answer because it is the most important outcome of effective risk treatment, as it ensures that the risk is managed in accordance with the organization's risk appetite and tolerance" (p. 28). Additionally, the Not All Risk Treatment Options Are the Same article from the ISACA Journal 2021 states that "risk treatment is the process of implementing corrective actions to address the root causes of the risk and to reduce the likelihood and/or impact of the risk" (p. 1)1.

Question: 481

Which of the following tools provides an incident response team with the GREATEST insight into insider threat activity across multiple systems?

A. A security information and event management (SIEM) system
B. An intrusion prevention system (IPS)
C. A virtual private network (VPN) with multi-factor authentication (MFA)
D. An identity and access management (IAM) system

Answer: A

Explanation:

A SIEM system is the best tool for providing an incident response team with the greatest insight into insider threat activity across multiple systems because it can collect, correlate, analyze, and report on security events and logs from various sources, such as network devices, servers, applications, and user activities. A SIEM system can also detect and alert on anomalous or suspicious behaviors, such as unauthorized access, data exfiltration, privilege escalation, or policy violations, that may indicate an insider threat. A SIEM system can also support forensic investigations and incident response actions by providing a centralized and comprehensive view of the security posture and incidents. Reference: The CISM Review Manual 2023 defines SIEM as "a technology that provides real-time analysis of security alerts generated by network hardware and applications" and states that "SIEM systems can help identify insider threats by correlating user activity logs with other security events and detecting deviations from normal patterns" (p. 184). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A security information and event management (SIEM) system is the correct answer because it can provide the most insight into insider threat activity across multiple systems by collecting, correlating, analyzing, and reporting on security events and logs from various sources" (p. 95). Additionally, the Detecting and Identifying Insider Threats article from the CISA website states that "threat detection and

identification is the process by which persons who might present an insider threat risk due to their observable, concerning behaviors come to the attention of an organization or insider threat team. Detecting and identifying potential insider threats requires both human and technological elements" and that "technological elements include tools such as security information and event management (SIEM) systems, user and entity behavior analytics (UEBA) systems, and data loss prevention (DLP) systems, which can monitor, analyze, and alert on user activities and network events" (p. 1)1.

Question: 482

Which of the following would BEST mitigate accidental data loss events?

A. Conduct periodic user awareness training.
B. Obtain senior management support for the information security strategy.
C. Conduct a data loss prevention (DLP) audit.
D. Enforce a data hard drive encryption policy.

Answer: A

Explanation:

Conducting periodic user awareness training is the best way to mitigate accidental data loss events because it can educate the users on the causes, consequences, and prevention of data loss, and increase their awareness of the security policies and procedures of the organization. User awareness training can also help users to identify and report potential data loss incidents, and to adopt good practices such as backing up data, encrypting data, and using secure channels for data transmission and storage.

Reference: The article Mistakes Happen—Mitigating Unintentional Data Loss from the ISACA Journal 2018 states that "user awareness training is the most effective way to prevent unintentional data loss" and that "user awareness training should include information on the types and sources of data loss, the impact and cost of data loss, the legal and regulatory requirements for data protection, the organization's data security policies and procedures, the roles and responsibilities of users in data security, the best practices and tools for data security, and the reporting and escalation process for data loss incidents" (p. 2)1. The Data Spill Management Guide from the Cyber.gov.au website also states that "user awareness training is an important preventative measure to reduce the likelihood of data spills" and that "user awareness training should cover topics such as data classification, data handling, data storage, data transmission, data disposal, and data spill reporting" (p. 2)

Question: 483

Which of the following is the PRIMARY reason to assign a risk owner in an organization?

A. To remediate residual risk

B. To define responsibilities C. To ensure accountability D. To identify emerging risk

Answer: C

Explanation:

The primary reason to assign a risk owner in an organization is to ensure accountability for the risk and its treatment. A risk owner is a person or entity that has the authority and responsibility to manage a specific risk and to implement the appropriate risk response actions. By assigning a risk owner, the organization can ensure that the risk is monitored, reported, and controlled in accordance with the organization's risk appetite and tolerance.

Reference: The CISM Review Manual 2023 defines risk owner as "the person or entity with the accountability and authority to manage a risk" and states that "the risk owner is responsible for ensuring that the risk is treated in a manner consistent with the enterprise's risk appetite and tolerance" (p. 93). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "To ensure accountability is the correct answer because it is the primary reason to assign a risk owner in an organization, as it ensures that the risk and its treatment are managed by a person or entity that has the authority and responsibility to do so" (p. 29). Additionally, the article Risk Ownership: The First Step of Effective Risk Management from the ISACA Journal 2019 states that "risk ownership is the first and most important step of effective risk management" and that "risk ownership ensures that there is clear accountability and responsibility for each risk and that risk owners are empowered to make risk decisions and implement risk responses" (p. 1)

Question: 484

Which of the following should be the GREATEST consideration when determining the recovery time objective (RTO) for an in-house critical application, database, or server?

A. Impact of service interruption
B. Results of recovery testing
C. Determination of recovery point objective (RPO)
D. Direction from senior management

Answer: A

Explanation:

Question: 485

Which of the following is the BEST way to ensure the business continuity plan (BCP) is current?

A. Manage business process changes.
B. Update business impact analyses (BIAs) on a regular basis.
C. Conduct periodic testing.
D. Review and update emergency contact lists.

Answer: C

Explanation:

Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.

Reference: The CISM Review Manual 2023 states that “testing is a critical component of the BCP process” and that “testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations” (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: “Conducting periodic testing is the correct answer because it is the best way to ensure the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update” (p. 98). Additionally, the article Business Continuity Planning: Testing an Organization’s Plan from the ISACA Journal 2019 states that “testing is essential to ensure that the BCP is current and effective” and that “testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks” (p. 1)

Question: 486

An organization's information security manager reads on social media that a recently purchased vendor product has been compromised and customer data has been posted online. What should the information security manager do FIRST?

A. Perform a business impact analysis (BIA).
B. Notify local law enforcement agencies of a breach.
C. Activate the incident response program.
D. Validate the risk to the organization.

Answer: D

Explanation:

The first thing that the information security manager should do after reading about a vendor product compromise on social media is to validate the risk to the organization. This means verifying the source and credibility of the information, determining if the organization uses the affected product, and assessing the potential impact and likelihood of the compromise on the organization's data and systems. Validating the risk to the organization will help the information security manager to decide on the appropriate course of action, such as activating the incident response program, notifying relevant stakeholders, or performing a BIA.
Reference: The CISM Review Manual 2023 states that "the information security manager is responsible for identifying and assessing the risks associated with the use of third-party products and services" and that "the information security manager should monitor and review the security performance and incidents of third-party products and services on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Validating the risk to the organization is the correct answer because it is the first and most important step to take after reading about a vendor product compromise on social media, as it will help the information security manager to confirm the accuracy and relevance of the information, and to evaluate the potential consequences and probability of the compromise on the organization's data and systems" (p. 63). Additionally, the article Defending Against Software Supply Chain Attacks from the CISA website states that "the first step in responding to a software supply chain attack is to validate the risk to the organization by verifying the source and credibility of the information, determining if the organization uses the affected software, and assessing the potential impact and likelihood of the compromise on the organization's data and systems" (p. 2)

Question: 487

When integrating security risk management into an organization it is MOST important to ensure:

A. business units approve the risk management methodology.
B. the risk treatment process is defined.
C. information security policies are documented and understood.
D. the risk management methodology follows an established framework.

Answer: A

Explanation:

When integrating security risk management into an organization, it is most important to ensure that the risk management methodology follows an established framework, such as ISO 31000, NIST SP 800-30, or COBIT.

This is because a framework provides a consistent and structured approach to identify, assess, treat, and monitor risks, and to align the risk management process with the organization's objectives, culture, and governance. A framework also helps to ensure compliance with relevant standards and regulations, and to facilitate communication and reporting of risks to stakeholders.
Reference: The CISM Review Manual 2023 states that "the risk management methodology should

follow an established framework that provides a consistent and structured approach to risk management" and that "the framework should be aligned with the enterprise's objectives, culture, and governance, and should comply with applicable standards and regulations" (p. 94). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "The risk management methodology follows an established framework is the correct answer because it is the most important factor to ensure the successful integration of security risk management into an organization, as it provides a common language and process for managing risks across the organization" (p. 29). Additionally, the article Integrating Risk Management into Business Processes from the ISACA Journal 2018 states that "a risk management framework provides a systematic and comprehensive approach to risk management that covers the entire risk management cycle, from risk identification to risk monitoring and reporting" and that "a risk management framework should be aligned with the organization's strategy, culture, and governance, and should follow recognized standards and best practices, such as ISO 31000, NIST SP 800-30, or COBIT" (p. 1)

Question: 488

What is the PRIMARY objective of implementing standard security configurations?

A. Maintain a flexible approach to mitigate potential risk to unsupported systems.
B. Minimize the operational burden of managing and monitoring unsupported systems.
C. Control vulnerabilities and reduce threats from changed configurations.
D. Compare configurations between supported and unsupported systems.

Answer: C

Explanation:

The primary objective of implementing standard security configurations is to control vulnerabilities and reduce threats from changed configurations. Standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices. By implementing standard security configurations, the organization can ensure that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected. This can help to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks.
Reference: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should establish and implement standard security configurations for information systems and devices, and monitor and review the security configuration on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Control vulnerabilities and reduce threats from changed configurations is the correct answer

because it is the primary objective of implementing standard security configurations, as it helps to maintain the security posture and functionality of information systems and devices, and to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks" (p. 63). Additionally, the article Standard Security Configurations from the ISACA Journal 2017 states that "standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices" and that "standard security configurations can help to control vulnerabilities and reduce threats from changed configurations by ensuring that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected" (p. 1)

Question: 489

An organization has identified a large volume of old data that appears to be unused. Which of the following should the information security manager do NEXT?

A. Consult the record retention policy.
B. Update the awareness and training program.
C. Implement media sanitization procedures.
D. Consult the backup and recovery policy.

Answer: A

Explanation:

The next thing that the information security manager should do after identifying a large volume of old data that appears to be unused is to consult the record retention policy. The record retention policy is a document that defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes. By consulting the record retention policy, the information security manager can determine if the old data is still required to be stored, archived, or disposed of, and how to do so in a secure and compliant manner. Reference: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the data lifecycle management process is in alignment with the organization's record retention policy" and that "the record retention policy defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes" (p. 140). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Consult the record retention policy is the correct answer because it is the next logical step to take after identifying a large volume of old data that appears to be unused, as it will help the information security manager to decide on the appropriate data lifecycle management actions for the old data, such as storage, archiving, or disposal" (p. 64). Additionally, the article Data Retention Policy: What It Is and How to Create One from the ISACA Journal 2019 states that "a data retention policy is a document that outlines the types, formats, and retention periods of data that an organization needs to keep for various purposes, such as legal compliance, business operations, or historical records" and that "a data retention policy can help an organization to manage its data lifecycle, optimize its storage capacity, reduce its costs, and enhance its security and privacy" (p. 1)1.

Question: 490

When an organization experiences a disruptive event, the business continuity plan (BCP) should be triggered PRIMARILY based on:

A. expected duration of outage.
B. management direction.
C. type of security incident.
D. the root cause of the event.

Answer: A

Explanation:

The expected duration of outage is the primary factor that should trigger the BCP because it indicates how long the organization can tolerate the disruption of its critical business processes and functions before it causes unacceptable consequences. The expected duration of outage is determined by the recovery time objectives (RTOs) that are defined for each critical business process and function based on the business impact analysis (BIA). The BCP should be triggered when the expected duration of outage exceeds or is likely to exceed the RTOs.

Reference: The CISM Review Manual 2023 defines RTO as "the maximum acceptable time that a service can be unavailable or disrupted before it causes unacceptable consequences" and states that "the RTO is determined based on the impact of service interruption on the enterprise's business processes, reputation, customers, and stakeholders" (p. 189). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Expected duration of outage is the correct answer because it is the primary factor that should trigger the BCP, as it reflects the maximum time that the organization can afford to lose its critical business processes and functions without causing unacceptable consequences" (p. 96). Additionally, the article Invoking your business continuity plan: five triggers, six decision points from the ITWeb website states that "the expected duration of outage is the most important consideration when deciding to invoke the BCP, as it indicates how long the organization can sustain the disruption before it impacts its business objectives, operations, reputation, and legal obligations" (p. 2)

Question: 491

Which of the following BEST indicates the effectiveness of the vendor risk management process?

A. Increase in the percentage of vendors certified to a globally recognized security standard
B. Increase in the percentage of vendors with a completed due diligence review
C. Increase in the percentage of vendors conducting mandatory security training
D. Increase in the percentage of vendors that have reported security breaches

Answer: A

Explanation:

This answer best indicates the effectiveness of the vendor risk management process because it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices. A globally recognized security standard, such as ISO 27001, NIST CSF, or COBIT, provides a comprehensive and objective framework for assessing and improving the security posture and performance of vendors.

Reference: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security requirements and expectations for third-party products and services are defined, communicated, and enforced" and that "the information security manager should verify that the third parties have implemented adequate security controls and practices, and that they comply with applicable standards and regulations" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Increase in the percentage of vendors certified to a globally recognized security standard is the correct answer because it best indicates the effectiveness of the vendor risk management process, as it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices" (p. 63). Additionally, the article Vendor Risk Management Demystified from the ISACA Journal 2015 states that "a globally recognized security standard provides a common language and framework for evaluating and improving the security posture and performance of vendors" and that "a vendor certification to a globally recognized security standard can help to reduce the risk of security breaches, increase the trust and confidence of customers and stakeholders, and enhance the reputation and competitiveness of the vendor" (p. 3

Question: 492

Which type of recovery site is MOST reliable and can support stringent recovery requirements?

A. Cold site
B. Warm site
C. Hot site
D. Mobile site

Answer: C

Explanation:

A hot site is the most reliable type of recovery site and can support stringent recovery requirements because it is a fully operational facility that mirrors the primary production center. A hot site has all the hardware, software, data, network, and personnel ready to resume the critical business functions within minutes of a disruptive event. A hot site also has backup power, security, and communication systems to ensure the continuity of operations.

Reference: The CISM Review Manual 2023 defines a hot site as "a fully operational facility that mirrors the primary production center" and states that "a hot site can support stringent recovery requirements and provide the shortest recovery time" (p. 190). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A hot site is the correct answer because it is the

most reliable type of recovery site and can support stringent recovery requirements, as it is a fully operational facility that mirrors the primary production center and can resume the critical business functions within minutes of a disruptive event" (p. 96). Additionally, the web search result 1 states that "the recovery site can be hot, warm, cold or mobile. Hot sites are facilities that mirror the primary production center" and that "hot sites are the most reliable and can support stringent recovery requirements" (p. 1).

Question: 493

To effectively manage an organization's information security risk, it is MOST important to:

A. assign risk management responsibility to an experienced consultant.
B. periodically identify and correct new systems vulnerabilities.
C. establish and communicate risk tolerance.
D. benchmark risk scenarios against peer organizations.

Answer: C

Explanation:

To effectively manage an organization's information security risk, it is most important to establish and communicate risk tolerance, which is the level of risk that the organization is willing to accept or bear. By establishing and communicating risk tolerance, the organization can align its risk management strategy and objectives with its business goals and values, and ensure that the risk management activities and decisions are consistent and appropriate across the organization.
Reference: The CISM Review Manual 2023 defines risk tolerance as "the acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives" and states that "the information security manager should assist the enterprise in establishing and communicating its risk tolerance, and ensure that the risk management process is aligned with the enterprise's risk tolerance" (p. 94). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Establish and communicate risk tolerance is the correct answer because it is the most important factor to effectively manage an organization's information security risk, as it helps to define the scope, direction, and priorities of the risk management process, and to ensure that the risk management activities and decisions are consistent and appropriate across the organization" (p. 29). Additionally, the article Risk Tolerance: The Forgotten Factor from the ISACA Journal 2019 states that "risk tolerance is the key factor that influences the risk management process and outcomes" and that "risk tolerance should be established and communicated by the organization's senior management and board of directors, and

should reflect the organization's strategy, culture, and governance" (p. 1)1

Question: 494

In order to gain organization-wide support for an information security program, which of the following is MOST important to consider?

A. Maturity of the security policy
B. Clarity of security roles and responsibilities
C. Corporate culture
D. Corporate risk framework

Answer: C

Explanation:

Corporate culture is the most important factor to consider when trying to gain organization-wide support for an information security program because it reflects the values, beliefs, and behaviors of the organization and its members. Corporate culture influences how the organization perceives, prioritizes, and responds to information security risks and issues, and how it adopts and implements information security policies and practices. By understanding and aligning with the corporate culture, the information security manager can communicate the benefits and value of the information security program, and foster a positive and collaborative security culture across the organization. Reference: The CISM Review Manual 2023 states that "corporate culture is the set of shared values, beliefs, and behaviors that characterize the organization and its members" and that "corporate culture affects how the organization views and manages information security risks and issues, and how it supports and implements information security policies and practices" (p. 81). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Corporate culture is the correct answer because it is the most important factor to consider when trying to gain organization-wide support for an information security program, as it reflects the values, beliefs, and behaviors of the organization and its members, and influences how they perceive, prioritize, and respond to information security risks and issues, and how they adopt and implement information security policies and practices" (p. 23). Additionally, the article Building a Culture of Security from the ISACA Journal 2019 states that "corporate culture is the key factor that determines the success or failure of an information security program" and that "corporate culture can be either an enabler or a barrier for information security, depending on how well it aligns with the information security objectives, values, and practices of the organization" (p. 1)

Question: 495

Which of the following provides the MOST useful information for identifying security control gaps on an application server?

A. Risk assessments
B. Threat models
C. Penetration testing
D. Internal audit reports

Answer: C

Explanation:

Penetration testing is the most useful method for identifying security control gaps on an application server because it simulates real-world attacks and exploits the vulnerabilities and weaknesses of the application

server. Penetration testing can reveal the actual impact and risk of the security control gaps, and provide recommendations for remediation and improvement.
Reference: The CISM Review Manual 2023 defines penetration testing as “a method of evaluating the security of an information system or network by simulating an attack from a malicious source” and states that “penetration testing can help identify security control gaps and provide evidence of the potential impact and risk of the gaps” (p. 185). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: “Penetration testing is the correct answer because it is the most useful method for identifying security control gaps on an application server, as it simulates real-world attacks and exploits the vulnerabilities and weaknesses of the application server, and provides recommendations for remediation and improvement” (p. 95).
Additionally, the web search result 4 states that “penetration testing is a valuable tool for discovering security gaps in your application server and network infrastructure” and that “penetration testing can help you assess the effectiveness and efficiency of your security controls, and identify the areas that need improvement or enhancement” (p. 1).

Question: 496

Which of the following would be MOST helpful when creating information security policies?

A. The information security framework
B. Business impact analysis (BIA)
C. Information security metrics
D. Risk assessment results

Answer: A

Explanation:

The information security framework is a set of principles, standards, guidelines, and best practices that define the scope, objectives, and requirements for information security in an organization. The information security framework is most helpful when creating information security policies because

it provides a consistent and coherent approach to managing information security risks, aligning with business goals and strategy, and complying with relevant laws and regulations. The information security framework also helps to establish the roles, responsibilities, and accountability of all stakeholders involved in information security governance, management, and operations.
Reference = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1: Information Security Framework2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1

Question: 497

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

A. Legal
B. Information security
C. Help desk
D. Human resources (HR)

Answer: B

Explanation:

Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. Reference = CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner."
SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process."
IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access."

Human resources (HR) is the most critical function when initiating the removal of system access for terminated employees because it is responsible for notifying the relevant parties, such as

information security, help desk, and legal, of the employee's termination status and date. HR also ensures that the employee's exit process is completed and documented, and that the employee returns any company-owned devices or assets. HR also coordinates with the employee's manager and team to ensure a smooth transition of work and responsibilities.

Question: 498

What should be the GREATEST concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider?

A. Vendor service level agreements (SLAs)
B. Independent review of the vendor
C. Local laws and regulations
D. Backup and restoration of data

Answer: C

Explanation:

he greatest concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider is the local laws and regulations that may apply to the data and the cloud service provider. Local laws and regulations may vary significantly across different jurisdictions and may impose different requirements or restrictions on the data protection, privacy, security, sovereignty, retention, disclosure, transfer, or access. These laws and regulations may also create potential conflicts or inconsistencies with the organization's own policies, standards, or contractual obligations. Therefore, an information security manager should conduct a thorough legal and regulatory analysis before outsourcing data processing to a cloud service provider and ensure that the cloud service provider complies with all the applicable laws and regulations in the relevant jurisdictions.
Reference = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1: Outsourcing2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1

Outsourcing data processing to a cloud service provider may expose the organization to different legal and regulatory requirements depending on the location of the data and the vendor. This could affect the organization's compliance and liability in case of a breach or dispute. Therefore, the information security manager should be most concerned about the local laws and regulations that apply to the outsourcing arrangement.

Question: 499

Which of the following is the MOST important outcome of a post-incident review?

A. The impact of the incident is reported to senior management.
B. The system affected by the incident is restored to its prior state.
C. The person responsible for the incident is identified.
D. The root cause of the incident is determined.

Answer: D

Explanation:

Determining the root cause of the incident is essential for preventing or minimizing the recurrence of similar incidents, as well as for identifying and implementing corrective actions to improve the security posture of the organization.
Reference = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.3

Question: 500

When establishing metrics for an information security program, the BEST approach is to identify indicators that:

A. reduce information security program spending.
B. support major information security initiatives.
C. reflect the corporate risk culture.
D. demonstrate the effectiveness of the security program.

Answer: D

Explanation:

Metrics for an information security program should be aligned with the security objectives and strategy, and should demonstrate how well the program is performing in terms of reducing risk, enhancing security posture, and supporting business goals. Metrics that support major information security initiatives, reflect the corporate risk culture, or reduce information security program spending may be useful, but they are not the best approach for establishing metrics for the entire program.

Reference = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112

Question: 501

Which of the following is MOST important to the effectiveness of an information security program?

A. Security metrics
B. Organizational culture
C. IT governance
D. Risk management

Answer: D

Explanation:

Risk management is the most important factor for the effectiveness of an information security program, as it provides a systematic and consistent approach to identify, assess, treat, and monitor the information security risks that could affect the organization's objectives. Risk management also helps to align the security program with the business strategy, prioritize the security initiatives and resources, and communicate the value of security to the stakeholders.

Reference = CISM Review Manual 2022, page 3071; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.1

Question: 502

Which of the following eradication methods is MOST appropriate when responding to an incident resulting in malware on an application server?

A. Disconnect the system from the network.

B. Change passwords on the compromised system.
C. Restore the system from a known good backup.
D. Perform operation system hardening.

Answer: C

Explanation:

Restoring the system from a known good backup is the most appropriate eradication method when responding to an incident resulting in malware on an application server, as it ensures that the system is free of any malicious code and that the data and applications are consistent with the expected state. Disconnecting the system from the network may prevent further spread of the malware, but it does not eradicate it from the system. Changing passwords on the compromised system may reduce the risk of unauthorized access, but it does not remove the malware from the system. Performing operation system hardening may improve the security configuration of the system, but it does not guarantee that the malware is eliminated from the system.
Reference = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.4

Question: 503

Which of the following is MOST important to include in an information security strategy?

A. Stakeholder requirements
B. Risk register
C. Industry benchmarks
D. Regulatory requirements

Answer: A

Explanation:

Stakeholder requirements are the most important to include in an information security strategy, as they reflect the business needs, objectives, and expectations of the organization and its key stakeholders. Stakeholder requirements also help to align the information security strategy with the enterprise governance and the organizational culture. Risk register, industry benchmarks, and regulatory requirements are important inputs for the information security strategy, but they are not the most important to include.
Reference = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Task 1.12

Question: 504

An organization uses a security standard that has undergone a major revision by the certifying authority. The old version of the standard will no longer be used for organizations wishing to maintain their certifications. Which of the following should be the FIRST course of action?

A. Evaluate the cost of maintaining the certification.
B. Review the new standard for applicability to the business.
C. Modify policies to ensure new requirements are covered.
D. Communicate the new standard to senior leadership.

Answer: B

Explanation:

Reviewing the new standard for applicability to the business is the first course of action, as it helps to understand the changes, gaps, and impacts of the revision on the organization's security posture, compliance status, and business objectives. Evaluating the cost of maintaining the certification, modifying policies to ensure new requirements are covered, and communicating the new standard to senior leadership are important steps, but they should be done after reviewing the new standard for applicability to the business.

Reference = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.2

Question: 505

Which of the following is the MOST important reason for an organization to communicate to affected parties that a security incident has occurred?

A. To improve awareness of information security
B. To disclose the root cause of the incident
C. To increase goodwill toward the organization
D. To comply with regulations regarding notification

Answer: D

Explanation:

Complying with regulations regarding notification is the most important reason for an organization to communicate to affected parties that a security incident has occurred, as it helps to avoid legal penalties, fines, or sanctions that may result from failing to notify the relevant authorities, customers, or other stakeholders in a timely and appropriate manner. Additionally, complying with regulations regarding notification may also help to preserve the trust and reputation of the organization, as well as to facilitate the investigation and resolution of the incident.

Reference = CISM Review Manual 2022, page 3151; CISM Exam Content Outline, Domain 4, Task 4.5

Question: 506

Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of confidentiality?

A. Ensuring hashing of administrator credentials
B. Enforcing service level agreements (SLAs)
C. Ensuring encryption for data in transit
D. Utilizing a formal change management process

Answer: C

Explanation:

Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being

transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).
Reference = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

Question: 507

Which of the following BEST enables an organization to operate smoothly with reduced capacities when service has been disrupted?

A. Crisis management plan
B. Disaster recovery plan (DRP)
C. Incident response plan
D. Business continuity plan (BCP)

Answer: D

Explanation:

A business continuity plan (BCP) is the best option that enables an organization to operate smoothly with reduced capacities when service has been disrupted, as it defines the processes and procedures to maintain or resume critical business functions and minimize the impact of the disruption on the organization's objectives, customers, and stakeholders. A BCP also includes strategies for resource management, communication, recovery, and testing.

Reference = CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity and Disaster Recovery Plans4

Question: 508

Following a breach where the risk has been isolated and forensic processes have been performed, which of the following should be done NEXT?

A. Place the web server in quarantine.
B. Rebuild the server from the last verified backup.
C. Shut down the server in an organized manner.
D. Rebuild the server with relevant patches from the original media.

Answer: B

Explanation:

= After a breach where the risk has been isolated and forensic processes have been performed, the next step should be to rebuild the server from the last verified backup. This will ensure that the server is restored to a known and secure state, and that any malicious code or data that may have been injected or compromised by the attacker is removed. Rebuilding the server from the original media may not be sufficient, as it may not include the latest patches or configurations that were applied before the breach. Placing the web server in quarantine or shutting it down may not be feasible or desirable, as it may disrupt the business operations or services that depend on the server. Rebuilding the server from the last verified backup is the best option to resume normal operations while maintaining security. Reference =
CISM Review Manual 15th Edition, page 118: "Recovery is the process of restoring normal operations after an incident. Recovery activities may include rebuilding systems, restoring data, applying patches, changing passwords, and testing functionality."
Data Breach Experts Share The Most Important Next Step You Should Take After A Data Breach in 2014 & 2015, snippet: "Restore from backup. If you have a backup of your system from before the breach, wipe your system clean and restore from backup. This will ensure that any backdoors or malware installed by the hackers are removed."

Question: 509

Which of the following should be done FIRST once a cybersecurity attack has been confirmed?

A. Isolate the affected system.
B. Notify senior management.
C. Power down the system.
D. Contact legal authorities.

Answer: A

Explanation:

Isolating the affected system is the first step in the incident response process, as it helps to contain the attack, prevent further damage, and preserve the evidence for analysis. Isolating the system can be done by disconnecting it from the network, blocking the malicious traffic, or applying quarantine rules.
Reference = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.22; Cybersecurity Incident Response Exercise Guidance3

Question: 510

An organization is about to purchase a rival organization. The PRIMARY reason for performing

information security due diligence prior to making the purchase is to:

A. determine the security exposures.
B. assess the ability to integrate the security department operations.
C. ensure compliance with international standards.
D. evaluate the security policy and standards.

Answer: A

Explanation:

Information security due diligence is the process of assessing the current state of information security in an organization, identifying any gaps, risks, or vulnerabilities, and estimating the costs and efforts required to remediate them. Performing information security due diligence prior to making the purchase is important to determine the security exposures that may affect the value, reputation, or liability of the organization, as well as the feasibility and compatibility of integrating the security systems and processes of the two organizations.
Reference = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Information Security Due Diligence Questionnair

Question: 511

Which of the following BEST demonstrates that an anti-phishing campaign is effective?

A. Improved staff attendance in awareness sessions
B. Decreased number of phishing emails received
C. Improved feedback on the anti-phishing campaign
D. Decreased number of incidents that have occurred

Answer: D

Explanation:

The ultimate goal of an anti-phishing campaign is to reduce the risk and impact of phishing attacks on the organization. Therefore, the most relevant and reliable indicator of the effectiveness of an anti-phishing campaign is the decreased number of incidents that have occurred as a result of phishing. This metric shows how well the employees have learned to recognize and report phishing emails, and how well the security controls have prevented or mitigated the damage caused by phishing.

Reference = Five Ways to Achieve a Successful Anti-Phishing Campaign; Don't click: towards an effective anti-phishing training. A comparative literature review; CISA, NSA, FBI, MS-ISAC Publish Guide on Preventing Phishing Intrusions

Question: 512

An organization that conducts business globally is planning to utilize a third-party service provider to process payroll information. Which of the following issues poses the GREATEST risk to the organization?

A. The third party does not have an independent assessment of controls available for review.
B. The third party has not provided evidence of compliance with local regulations where data is generated.
C. The third-party contract does not include an indemnity clause for compensation in the event of a breach.
D. The third party's service level agreement (SLA) does not include guarantees of uptime.

Answer: B

Explanation:

The third party's lack of compliance with local regulations poses the greatest risk to the organization, as it may expose the organization to legal, regulatory, or reputational consequences, such as fines, sanctions, lawsuits, or loss of customer trust. Payroll information is considered sensitive personal data that may be subject to different privacy and security laws depending on the jurisdiction where it is generated, processed, or stored. Therefore, the organization should ensure that the third party adheres to the applicable regulations and standards, and obtains the necessary certifications or attestations to demonstrate compliance.

Reference = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Ensuring Vendor Compliance and Third-Party Risk Mitigation; How to Manage Access Risk Regarding Third-Party Service Providers

Question: 513

Capacity planning would prevent:

A. file system overload arising from distributed denial of service (DDoS) attacks.

B. system downtime for scheduled security maintenance.
C. application failures arising from insufficient hardware resources.
D. software failures arising from exploitation of buffer capacity vulnerabilities.

Answer: C

Explanation:

Capacity planning is the process of estimating and allocating the required resources (such as CPU, memory, disk space, bandwidth, etc.) to meet the current and future demands of the information systems and applications. Capacity planning would prevent application failures arising from insufficient hardware resources, as it would ensure that the applications have enough resources to function properly and efficiently, and avoid performance degradation, errors, or crashes.
Reference = CISM Review Manual 2022, page 3081; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.92; What is Capacity Planning? Definition and Examples

Question: 514

Which of the following is the BEST indication of a mature information security program?

A. Security incidents are managed properly.
B. Security spending is below budget.
C. Security resources are optimized.
D. Security audit findings are reduced.

Answer: C

Explanation:

A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human, financial, and technical resources in the most efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.
Reference = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

Question: 515

Which of the following is the PRIMARY benefit of implementing an information security governance framework?

A. The framework defines managerial responsibilities for risk impacts to business goals.
B. The framework provides direction to meet business goals while balancing risks and controls.
C. The framework provides a roadmap to maximize revenue through the secure use of technology.
D. The framework is able to confirm the validity of business goals and strategies.

Answer: B

Explanation:

An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs, priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified.
Reference = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

Question: 516

Which of the following is MOST important for guiding the development and management of a comprehensive information security program?

A. Adopting information security program management best practices
B. Implementing policies and procedures to address the information security strategy
C. Aligning the organization's business objectives with IT objectives
D. Establishing and maintaining an information security governance framework

Answer: D

Explanation:

An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs, priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified.
Reference = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

Question: 517

The information security manager of a multinational organization has been asked to consolidate the

information security policies of its regional locations. Which of the following would be of GREATEST concern?

A. Varying threat environments
B. Disparate reporting lines
C. Conflicting legal requirements D. Differences in work culture

Answer: C

Explanation:

Conflicting legal requirements would be of greatest concern when consolidating the information security policies of regional locations, as they may pose significant challenges and risks for the organization's compliance, privacy, and data protection obligations. Different jurisdictions may have different laws and regulations regarding information security, such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. These laws and regulations may have different definitions, scopes, standards, and enforcement mechanisms for information security, which may create conflicts or inconsistencies when applying a unified policy across the organization. Therefore, the information security manager should conduct a thorough analysis of the legal requirements of each location, and ensure that the consolidated policy meets the highest level of compliance and avoids any violations or penalties. Reference = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; CISM 2020: IT Security Policies; Information Security Due Diligence Questionnaire

Question: 518

Which of the following should be the FIRST step in patch management procedures when receiving an emergency security patch?

A. Schedule patching based on the criticality.
B. Install the patch immediately to eliminate the vulnerability.
C. Conduct comprehensive testing of the patch.
D. Validate the authenticity of the patch.

Answer: D

Explanation:

Validating the authenticity of the patch is the first step in patch management procedures when receiving an emergency security patch, as it helps to ensure that the patch is genuine and not malicious. Validating the authenticity of the patch can be done by verifying the source, signature, checksum, or certificate of the patch, and comparing it with the information provided by the software vendor or manufacturer. Installing an unverified patch may introduce malware, compromise the system, or cause unexpected errors or conflicts.

Reference = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.42; Practical Patch Management and Mitigation1; Vulnerability and patch management in the CISSP exam3

Question: 519

A recent audit found that an organization's new user accounts are not set up uniformly. Which of the following is MOST important for the information security manager to review?

A. Automated controls
B. Security policies
C. Guidelines
D. Standards

Answer: D

Explanation:

Standards are the most important thing to review, as they define the specific and mandatory requirements for setting up new user accounts, such as the naming conventions, access rights, password policies, and expiration dates. Standards help to ensure consistency, security, and compliance across the organization's information systems and users. If the standards are not followed, the organization may face increased risks of unauthorized access, data breaches, or audit failures.

Reference = CISM Review Manual 2022, page 341; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.32; CISM 2020: IT Security Policies; Information Security Policy, Standards, and Guidelines

Question: 520

Which of the following is the BEST course of action when confidential information is inadvertently disseminated outside the organization?

A. Review compliance requirements.
B. Communicate the exposure.
C. Declare an incident.
D. Change the encryption keys.

Answer: C

Explanation:

Declaring an incident is the best course of action when confidential information is inadvertently disseminated outside the organization, as it triggers the incident response process, which aims to contain, analyze, eradicate, recover, and learn from the incident. Declaring an incident also helps to communicate the exposure to the

relevant stakeholders, such as senior management, legal authorities, customers, or regulators, and to comply with the applicable laws and regulations regarding notification and disclosure. Changing the encryption keys, reviewing compliance requirements, or communicating the exposure are possible steps within the incident response process, but they are not the first course of action.

Reference = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.12; CISM 2020: Incident Management; How to Respond to a Data Breach

Question: 521

Management would like to understand the risk associated with engaging an Infrastructure-as-a- Service (IaaS) provider compared to hosting internally. Which of the following would provide the BEST method of comparing risk scenarios?

A. Mapping risk scenarios according to sensitivity of data
B. Reviewing mitigating and compensating controls for each risk scenario
C. Mapping the risk scenarios by likelihood and impact on a chart
D. Performing a risk assessment on the IaaS provider

Answer: C

Explanation:

Mapping the risk scenarios by likelihood and impact on a chart is the best method of comparing risk scenarios, as it helps to visualize and prioritize the different types and levels of risks associated with each option. A chart can also facilitate the communication and decision-making process by showing the trade-offs and benefits of each option. A chart can be based on qualitative or quantitative data, depending on the availability and accuracy of the information.

Reference = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; A risk assessment model for selecting cloud service providers; Security best practices for IaaS workloads in Azure

Question: 522

A PRIMARY benefit of adopting an information security framework is that it provides:

A. credible emerging threat intelligence.
B. security and vulnerability reporting guidelines.
C. common exploitability indices.
D. standardized security controls.

Answer: D

Explanation:

A standardized security control is a set of rules, guidelines, or best practices that are designed to protect the confidentiality, integrity, and availability of information assets and systems. An information security framework is a collection of standardized security controls that are aligned with the organization's objectives, strategy, and risk appetite. Adopting an information security framework provides a primary benefit of ensuring consistency, efficiency, and effectiveness in the implementation and management of information security across the organization.
Reference = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is an Information Security Framework?; Information Security Frameworks: What Are They and Why Do You Need One?

Question: 523

Which of the following should be the GREATEST concern for an information security manager when an annual audit reveals the organization's business continuity plan (BCP) has not been reviewed or updated in more than a year?

A. An outdated BCP may result in less efficient recovery if an actual incident occurs.
B. The organization may suffer reputational damage for not following industry best practices.
C. The audit finding may impact the overall risk rating of the organization.
D. The lack of updates to the BCP may result in noncompliance with internal policies.

Answer: A

Explanation:

A BCP is a document that outlines the processes and procedures to maintain or resume critical business functions and minimize the impact of a disruption on the organization's objectives, customers, and stakeholders. A BCP should be reviewed and updated regularly to reflect the changes in the organization's environment, risks, resources, and requirements. An outdated BCP may result in less efficient recovery if an actual incident occurs, as it may not account for the current situation, dependencies, priorities, or recovery strategies. This may lead to increased downtime, losses, or damages for the organization.
Reference = CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity and Disaster Recovery Plans

Question: 524

Which of the following is the MOST appropriate metric to demonstrate the effectiveness of information security controls to senior management?

A. Downtime due to malware infections
B. Number of security vulnerabilities uncovered with network scans
C. Percentage of servers patched
D. Annualized loss resulting from security incidents

Answer: D

Explanation:

Annualized loss resulting from security incidents is the most appropriate metric to demonstrate the effectiveness of information security controls to senior management, as it quantifies the financial impact of security breaches on the organization's assets, operations, and reputation. This metric helps to communicate the value of security investments, justify the security budget, and prioritize the security initiatives based on the potential loss reduction. Annualized loss resulting from security incidents can be calculated by multiplying the annualized rate of occurrence (ARO) of an incident by the single loss expectancy (SLE) of an incident. ARO is the estimated frequency of an incident occurring in a year, and SLE is the estimated cost of an incident. For example, if an organization estimates that a ransomware attack may occur once every two years, and that each attack may cost $100,000 to recover, then the annualized loss resulting from ransomware attacks is $50,000 ($100,000 / 2).

Reference = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112; Key Performance Indicators for Security Governance, Part 1; Performance Measurement Guide for Information Security

Question: 525

An organization provides notebook PCs, cable wire locks, smartphone access, and virtual private network (VPN) access to its remote employees. Which of the following is MOST important for the information security manager to ensure?

A. Employees use smartphone tethering when accessing from remote locations.
B. Employees physically lock PCs when leaving the immediate area.
C. Employees are trained on the acceptable use policy.
D. Employees use the VPN when accessing the organization's online resources.

Answer: D

Explanation:

Using the VPN when accessing the organization's online resources is the most important thing to ensure, as it provides a secure and encrypted connection between the remote employees and the organization's network, and protects the data and systems from unauthorized access, interception, or tampering. VPNs also help to comply with the organization's security policies and standards, and to prevent data leakage or breaches.

Reference = CISM Review Manual 2022, page 3081; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.92; CISM 2020: Remote Access Security; How to Secure Remote Workers with VPN

Question: 526

The business value of an information asset is derived from:

A. the threat profile.
B. its criticality.
C. the risk assessment.
D. its replacement cost.

Answer: B

Explanation:

The business value of an information asset is derived from its criticality, which is the degree of importance or dependency of the asset to the organization's objectives, operations, and stakeholders. The criticality of an information asset can be determined by assessing its impact on the confidentiality, integrity, and availability (CIA) of the information, as well as its sensitivity, classification, and regulatory requirements. The higher the criticality of an information asset, the higher its business value, and the more resources and controls are needed to protect it.
Reference = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; IT Asset Valuation, Risk Assessment and Control Implementation Model1; Managing Data as an Asset3

Question: 527

Which of the following is the MOST important function of an information security steering committee?

A. Assigning data classifications to organizational assets B. Developing organizational risk assessment processes
C. Obtaining multiple perspectives from the business

D. Defining security standards for logical access controls

Answer: C

Explanation:

An information security steering committee is a group of senior executives and managers from different business units and functions who provide strategic direction, oversight, and support for the information security program. The most important function of the committee is to obtain multiple perspectives from the business, as this helps to ensure that the information security program aligns with the business goals, needs, and culture, and that the security decisions reflect the interests and expectations of the stakeholders.
Reference = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; Improve Security Governance With a Security Steering Committee2; The Role of the

Corporate Information Security Steering Committee3

Question: 528

An employee clicked on a malicious link in an email that resulted in compromising company dat a. What is the BEST way to mitigate this risk in the future?

A. Conduct phishing awareness training.
B. Implement disciplinary procedures.
C. Establish an acceptable use policy.
D. Assess and update spam filtering rules.

Answer: A

Explanation:

Phishing awareness training is the best way to mitigate the risk of employees clicking on malicious links in emails, as it educates them on how to recognize and avoid phishing attempts. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 179, section 4.3.2.2.

Question: 529

Which of the following is the PRIMARY purpose of a business impact analysis (BIA)?

A. To define security roles and responsibilities
B. To determine return on investment (ROI)
C. To establish incident severity levels
D. To determine the criticality of information assets

Answer: D

Explanation:

A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. The primary purpose of a BIA is to determine the criticality of information assets and the impact of their unavailability on the organization's mission, objectives and reputation. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

Question: 530

Which of the following is the MOST effective way to ensure information security policies are understood?

A. Implement a whistle-blower program.
B. Provide regular security awareness training.
C. Include security responsibilities in job descriptions.
D. Document security procedures.

Answer: B

Explanation:

Security awareness training is the most effective way to ensure information security policies are understood, as it educates employees on the purpose, content and importance of the policies, and how to comply with them. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

Question: 531

An organization has remediated a security flaw in a system. Which of the following should be done NEXT?

A. Assess the residual risk.
B. Share lessons learned with the organization.
C. Update the system's documentation.
D. Allocate budget for penetration testing.

Answer: A

Explanation:

Residual risk is the risk that remains after applying controls to mitigate the original risk. It is important to assess the residual risk after remediation to ensure that it is within the acceptable level and tolerance of the organization. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

Question: 532

Which is MOST important to identify when developing an effective information security strategy?

A. Security awareness training needs
B. Potential savings resulting from security governance
C. Business assets to be secured
D. Residual risk levels

Answer: C

Explanation:

Business assets are the resources that enable the organization to achieve its objectives and create value. Identifying the business assets to be secured is the most important step in developing an effective information security strategy, as it helps to align the security goals with the business goals, prioritize the security efforts and resources, and define the scope and boundaries of the security program. (From CISM Review Manual 15th Edition)

Reference: CISM Review Manual 15th Edition, page 27, section 1.2.1.

Question: 533

Which of the following presents the GREATEST risk associated with the use of an automated security information and event management (SIEM) system?

A. Low number of false positives
B. Low number of false negatives
C. High number of false positives
D. High number of false negatives

Answer: D

Explanation:

A false negative is a security incident that was not detected by the SIEM system, which presents the greatest risk as it allows attackers to compromise the organization's assets and data without being noticed or stopped. A high number of false negatives can indicate that the SIEM system is not configured properly, has insufficient data sources, or lacks effective analytics and correlation rules. (From CISM Review Manual 15th Edition)

Reference: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

Question: 534

A security incident has been reported within an organization. When should an information security manager contact the information owner?

A. After the incident has been contained
B. After the incident has been mitigated
C. After the incident has been confirmed
D. After the potential incident has been logged

Answer: C

Explanation:

The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

Question: 535

An organization recently updated and published its information security policy and standards. What should the information security manager do NEXT?

A. Conduct a risk assessment.
B. Communicate the changes to stakeholders.
C. Update the organization's risk register.
D. Develop a policy exception process.

Answer: B

Explanation:

Communicating the changes to stakeholders is the next step after updating and publishing the information security policy and standards, as it ensures that the stakeholders are aware of the new or revised requirements, expectations and responsibilities, and can provide feedback or raise concerns if needed. Communication also helps to promote the acceptance and adoption of the policy and standards, and to reinforce the security culture and awareness within the organization. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

Question: 536

Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?

A. Requiring an external security audit of the IT service provider

B. Requiring regular reporting from the IT service provider
C. Defining information security requirements with internal IT
D. Defining the business recovery plan with the IT service provider

Answer: B

Explanation:

Requiring regular reporting from the IT service provider is the best way to ensure compliance with the organization's information security requirements, as it allows the organization to monitor the performance, security incidents, service levels, and compliance status of the IT service provider. Reporting also helps to identify any gaps or issues that need to be addressed or resolved. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

Question: 537

Which of the following is the BEST indicator of the maturity level of a vendor risk management process?

A. Average time required to complete the vendor risk management process
B. Percentage of vendors that have gone through the vendor onboarding process
C. Percentage of vendors that are regularly reviewed against defined criteria
D. Number of vendors rejected because of security review results

Answer: C

Explanation:

The percentage of vendors that are regularly reviewed against defined criteria is the best indicator of the maturity level of a vendor risk management process, as it reflects the extent to which the organization has established and implemented a consistent, repeatable, and effective process to monitor and evaluate the security performance and compliance of its vendors. A high percentage indicates a mature process that covers all vendors and applies clear and relevant criteria based on the organization's risk appetite and objectives. A low percentage indicates a less mature process that may be ad hoc, incomplete, or outdated. (From CISM Review Manual 15th Edition) Reference: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

Question: 538

Which of the following should be the PRIMARY focus of a status report on the information security program to senior management?

A. Providing evidence that resources are performing as expected
B. Verifying security costs do not exceed the budget
C. Demonstrating risk is managed at the desired level
D. Confirming the organization complies with security policies

Answer: C

Explanation:

The primary focus of a status report on the information security program to senior management is to demonstrate that the risk to the organization's information assets is managed at the desired level, in alignment with the business objectives and risk appetite. This can be achieved by providing relevant and meaningful metrics, indicators, and trends that show the performance, effectiveness, and value of the information security program, as well as the current and emerging risks and the corresponding mitigation strategies. (From CISM Review Manual 15th Edition) Reference: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

Question: 539

Which of the following is the BEST indication that an organization has integrated information security governance with corporate governance?

A. Security performance metrics are measured against business objectives.
B. Impact is measured according to business loss when assessing IT risk.
C. Security policies are reviewed whenever business objectives are changed.
D. Service levels for security vendors are defined according to business needs.

Answer: A

Explanation:

Security performance metrics are quantitative or qualitative measures that indicate the effectiveness and efficiency of the information security program in achieving the organization's security goals and objectives. Measuring security performance metrics against business objectives is the best indication that an organization has integrated information security governance with corporate governance, as it demonstrates that the security program is aligned with and supports the business strategy, value delivery, and risk management. (From CISM Review Manual 15th Edition) Reference: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

Question: 540

Which of the following is the PRIMARY objective of a cyber resilience strategy?

A. Business continuity

B. Regulatory compliance
C. Employee awareness
D. Executive support

Answer: A

Explanation:

Business continuity is the primary objective of a cyber resilience strategy, as it aims to ensure that the organization can continue to deliver its essential products and services in the face of cyber disruptions, and recover to normal operations as quickly and effectively as possible. A cyber resilience strategy should align with the business continuity plan and support the organization's mission, vision, and values. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

Question: 541

Which of the following would BEST demonstrate the status of an organization's information security program to the board of directors?

A. Information security program metrics
B. Results of a recent external audit
C. The information security operations matrix
D. Changes to information security risks

Answer: A

Explanation:

Information security program metrics are the best way to demonstrate the status of an organization's information security program to the board of directors, as they provide relevant and meaningful information on the performance, effectiveness, and value of the program, as well as the current and emerging risks and the corresponding mitigation strategies. Information security program metrics should be aligned with the business objectives and risk appetite of the organization, and should be presented in a clear and concise manner that enables the board of directors to make informed decisions and provide oversight. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

Question: 542

When testing an incident response plan for recovery from a ransomware attack, which of the following is MOST important to verify?

A. Digital currency is immediately available.
B. Network access requires two-factor authentication.
C. Data backups are recoverable from an offsite location.
D. An alternative network link is immediately available.

Answer: C

Explanation:

Data backups are recoverable from an offsite location is the most important thing to verify when testing an incident response plan for recovery from a ransomware attack, as it ensures that the organization can restore its data and resume its operations without paying the ransom or losing critical information. Data backups should be performed regularly, stored securely, and tested for integrity and availability. (From CISM Review Manual 15th Edition) Reference: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

Question: 543

Which of the following elements of a service contract would BEST enable an organization to monitor the information security risk associated with a cloud service provider?

A. Indemnification clause
B. Breach detection and notification
C. Compliance status reporting
D. Physical access to service provider premises

Answer: C

Explanation:

Compliance status reporting is the best element of a service contract that would enable an organization to monitor the information security risk associated with a cloud service provider, as it provides the organization with regular and timely information on the cloud service provider's compliance with the agreed-upon security requirements, standards, and regulations. Compliance status reporting also helps the organization to identify any gaps or issues that need to be addressed or resolved, and to verify the effectiveness of the cloud service provider's controls. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

Question: 544

Which of the following is the MOST effective way to ensure the security of services and solutions delivered by third-party vendors?

A. Integrate risk management into the vendor management process.

B. Conduct security reviews on the services and solutions delivered.
C. Review third-party contracts as part of the vendor management process.
D. Perform an audit on vendors' security controls and practices.

Answer: A

Explanation:

Integrating risk management into the vendor management process is the most effective way to ensure the security of services and solutions delivered by third-party vendors, as it enables the organization to identify, assess, treat, and monitor the risks associated with outsourcing. Risk management should be applied throughout the vendor life cycle, from selection, contracting, onboarding, monitoring, to termination. Risk management also helps the organization to define the security requirements, expectations, and responsibilities for the vendors, and to evaluate their performance and compliance. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 184, section 4.3.3.2; Preparing Your First Supplier

Audit Plan1.

Question: 545

Who has the PRIMARY authority to decide if additional risk treatments are required to mitigate an identified risk?

A. Information security manager
B. IT risk manager
C. Internal auditor
D. Risk owner

Answer: D

Explanation:

The risk owner is the person who has the authority and accountability to make decisions about the risk, including whether to accept, avoid, transfer, or mitigate it. The risk owner is also responsible for implementing and monitoring the risk treatment plan and reporting on the risk status. The risk owner is usually the business process owner or the information owner of the asset affected by the risk. (From CISM Review Manual 15th Edition)
Reference: CISM Review Manual 15th Edition, page 64, section 2.2.1.2.

Question: 546

Which of the following is the MOST effective way to identify changes in an information security environment?

A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring

Answer: D

Explanation:

Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect

and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371)

Reference: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-1371, page 1, section 1.1.

Question: 547

While conducting a test of a business continuity plan (BCP), which of the following is the MOST important consideration?

A. The test is scheduled to reduce operational impact.
B. The test involves IT members in the test process.
C. The test addresses the critical components.
D. The test simulates actual prime-time processing conditions.

Answer: C

Explanation:

The test addresses the critical components is the most important consideration while conducting a test of a business continuity plan (BCP), as it ensures that the test covers the essential functions, processes, and resources that are required to maintain or resume the organization's operations in the event of a disruption. The test should also verify that the recovery objectives, such as recovery time objective (RTO) and recovery point objective (RPO), are met. (From CISM Review Manual 15th Edition)

Reference: CISM Review Manual 15th Edition, page 178, section 4.3.2.1; CISSP Exam Cram: Business Continuity and Disaster Recovery Planning1, page 5, section Testing the Plan.

Question: 548

An organization is considering the feasibility of implementing a big data solution to analyze customer dat a. In order to support this initiative, the information security manager should FIRST:

A. inventory sensitive customer data to be processed by the solution.
B. determine information security resource and budget requirements.
C. assess potential information security risk to the organization.
D. develop information security requirements for the big data solution.

Answer: C

Explanation:

Assessing potential information security risk to the organization is the first step that the information security manager should take when considering the feasibility of implementing a big data solution to analyze customer data, as it helps to identify and evaluate the threats, vulnerabilities, and impacts that may arise from the collection, processing, storage, and sharing of large volumes and varieties of customer data. Assessing risk also helps to determine the risk appetite and tolerance of the organization, and to prioritize the risk treatment options and security controls that are needed to protect the customer data and the big data solution. (From CISM Review Manual 15th Edition) Reference: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Big Data Security and Privacy Issues in Healthcare1, page 1, section 1. Introduction.

Question: 549

Prior to implementing a bring your own device (BYOD) program, it is MOST important to:

A. select mobile device management (MDM) software.
B. survey employees for requested applications.
C. develop an acceptable use policy.
D. review currently utilized applications.

Answer: C

Explanation:

Before implementing a BYOD program, it is most important to develop an acceptable use policy that defines the roles and responsibilities of the organization and the employees, the security requirements and controls for the devices, the acceptable and unacceptable behaviors and activities, and the consequences of non-compliance. This policy will help to establish a clear and consistent framework for managing the risks and benefits of BYOD.
Reference = CISM Review Manual, 16th Edition, page 197

Question: 550

Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?

A. Create a security exception.
B. Perform a gap analysis to determine needed resources.
C. Perform a vulnerability assessment.
D. Assess the risk to business operations.

Answer: D

Explanation:

The information security manager should first assess the risk to business operations that are caused by the information security issues reported by internal audit. This will help to prioritize the remediation actions and allocate the necessary resources. Creating a security exception, performing a gap analysis, or performing a vulnerability assessment are possible subsequent steps, but they are not the first action to take.
Reference = CISM Review Manual, 16th Edition, page 48

Question: 551

Which of the following is MOST important to the successful implementation of an information security program?

A. Adequate security resources are allocated to the program.
B. Key performance indicators (KPIs) are defined.
C. A balanced scorecard is approved by the steering committee.
D. The program is developed using global security standards.

Answer: A

Explanation:

The successful implementation of an information security program depends largely on the availability and allocation of adequate security resources, such as budget, staff, technology, and training. Without sufficient resources, the program may not be able to achieve its objectives, comply with the security strategy, or address the security risks. Key performance indicators (KPIs), a balanced scorecard, and global security standards are also important elements of an information security program, but they are not as critical as the resource allocation.
Reference = CISM Review Manual, 16th Edition, page 69

Question: 552

Which of the following is MOST important to consider when defining control objectives?

A. Industry best practices
B. An information security framework
C. Control recommendations from a recent audit
D. The organization's risk appetite

Answer: D

Explanation:

The organization’s risk appetite is the most important factor to consider when defining control objectives, because it reflects the amount and type of risk that the organization is willing to accept or avoid in pursuit of its goals. Control objectives should align with the risk appetite and support the achievement of the organization’s objectives. Industry best practices, an information security framework, and control recommendations from a recent audit are also useful sources of guidance, but they are not as critical as the risk appetite.
Reference = CISM Review Manual, 16th Edition, page 75

Question: 553

Which of the following should be the PRIMARY basis for establishing metrics that measure the effectiveness of an information security program?

A. Residual risk
B. Regulatory requirements
C. Risk tolerance
D. Control objectives

Answer: C

Explanation:

The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance.
Reference = CISM Review Manual, 16th Edition, page 69

Question: 554

During the selection of a Software as a Service (SaaS) vendor for a business process, the vendor provides evidence of a globally accepted information security certification. Which of the following is the MOST important consideration?

A. The certification includes industry-recognized security controls.
B. The certification was issued within the last five years.
C. The certification is issued for the specific scope.
D. The certification is easily verified.

Answer: C

Explanation:

The most important consideration when selecting a SaaS vendor for a business process is whether the vendor's information security certification is issued for the specific scope of the service that the organization needs. A certification that covers the entire vendor organization or a different service may not be relevant or sufficient for the organization's security requirements. The certification should also include industry-recognized security controls, be issued within a reasonable time frame, and be easily verified, but these are not as critical as the scope.

Reference = CISM Review Manual, 16th Edition, page 1841; 5 Top SaaS Security Certifications for SaaS Providers

Question: 555

Which of the following trends would be of GREATEST concern when reviewing the performance of an organization's intrusion detection systems (IDSs)?

A. Decrease in false positives
B. Increase in false positives
C. Increase in false negatives
D. Decrease in false negatives

Answer: C

Explanation:

An increase in false negatives would be of greatest concern when reviewing the performance of an organization's IDSs, because it means that the IDSs are failing to detect and alert on actual attacks that are occurring on the network. False negatives can lead to serious security breaches, data loss, reputational damage, and legal liabilities for the organization. False positives, on the other hand, are alerts that are triggered by benign or normal activities that are mistaken for attacks. False positives can cause annoyance, inefficiency, and desensitization, but they do not pose a direct threat to the security of the network. Therefore,

a decrease in false positives would be desirable, and an increase in false positives would be less concerning than an increase in false negatives.
Reference = CISM Review Manual, 16th Edition, page 2231; Intrusion Detection Systems | NIST

Question: 556

An information security manager notes that security incidents are not being appropriately escalated by the help desk after tickets are logged. Which of the following is the BEST automated control to resolve this issue?

A. Implementing automated vulnerability scanning in the help desk workflow
B. Changing the default setting for all security incidents to the highest priority
C. Integrating automated service level agreement (SLA) reporting into the help desk ticketing system D. Integrating incident response workflow into the help desk ticketing system

Answer: D

Explanation:

The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities. This will improve the efficiency, effectiveness, and consistency of the incident response process.
Reference = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

Question: 557

An internal audit has revealed that a number of information assets have been inappropriately classified. To correct the classifications, the remediation accountability should be assigned to:

A. the business users.
B. the information owners.
C. the system administrators.
D. senior management.

Answer: B

Explanation:

The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities. This will improve the efficiency, effectiveness, and consistency of the incident response process.

Reference = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

Question: 558

Which of the following roles is BEST suited to validate user access requirements during an annual

user access review?

A. Access manager
B. IT director
C. System administrator
D. Business owner

Answer: D

Explanation:

The business owner is the best suited role to validate user access requirements during an annual user access review, because the business owner is responsible for determining the business needs and objectives of the users, as well as defining the appropriate access rights and privileges for each user role. The business owner is also accountable for ensuring that the user access is aligned with the organization's policies and standards, and that the user access review is conducted effectively and efficiently1. The access manager, the IT director, and the system administrator are not as suitable as the business owner, because they are more involved in the technical and operational aspects of user access management, rather than the business aspects.

Reference = Effective User Access Reviews

Question: 559

When developing an incident escalation process, the BEST approach is to classify incidents based on:

A. estimated time to recover.
B. information assets affected.
C. recovery point objectives (RPOs).
D. their root causes.

Answer: B

Explanation:

The best approach to developing an incident escalation process is to classify incidents based on the information assets affected, because this will help to determine the impact and severity of the incidents, as well as the appropriate response and recovery actions. The information assets affected by an incident can indicate the potential loss of confidentiality, integrity, or availability of the information, as well as the legal, regulatory, contractual, or reputational implications. By classifying incidents based on the information assets affected, the organization can prioritize the incidents and escalate them to the relevant stakeholders and authorities.

Reference = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

Question: 560

Of the following, who is BEST positioned to be accountable for risk acceptance decisions based on risk appetite?

A. Information security manager
B. Chief risk officer (CRO)
C. Information security steering committee
D. Risk owner

Answer: D

Explanation:

The risk owner is the best positioned to be accountable for risk acceptance decisions based on risk appetite, because the risk owner is the person or entity with the accountability and authority to manage a risk1. The risk owner is responsible for evaluating the risk level, comparing it with the risk appetite, and deciding whether to accept, avoid, transfer, or mitigate the risk2. The risk owner is also accountable for monitoring and reporting on the risk status and outcomes3. The information security manager, the chief risk officer (CRO), and the information security steering committee may have some roles and responsibilities in the risk management process, but they are not the primary accountable parties for risk acceptance decisions.

Reference = CISM Review Manual, 16th Edition, page 754; Risk Acceptance

Question: 561

Which of the following should an information security manager do FIRST when there is a conflict between the organization's information security policy and a local regulation?

A. Enforce the local regulation.

B. Obtain legal guidance.
C. Enforce the organization's information security policy.
D. Obtain an independent assessment of the regulation.

Answer: B

Explanation:

The information security manager should first obtain legal guidance when there is a conflict between the organization's information security policy and a local regulation, because this will help to understand the implications and consequences of the conflict, and to identify the possible options

and solutions for resolving it. The information security manager should also consult with the relevant stakeholders, such as senior management, business owners, and information owners, to determine the best course of action that aligns with the organization's objectives, risk appetite, and compliance obligations. Enforcing the local regulation or the organization's information security policy without legal guidance may expose the organization to legal liabilities, security risks, or operational disruptions. Obtaining an independent assessment of the regulation may be helpful, but it is not the first step to take.

Reference = CISM Review Manual, 16th Edition, page 691; A Guide to ISACA CISM Domains & Domain 1: Information Security Governance2

Question: 562

An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

A. Internal IT audit
B. The data custodian
C. The information security manager
D. The data owner

Answer: D

Explanation:

The data owner is the person who has the authority and responsibility to classify, grant access, and monitor the use of the CRM data. The data owner should ensure that the data is protected according to its classification and business requirements. The data custodian is the person who implements the controls and procedures to protect the data as directed by the data owner. The information security manager is the person who advises the data owner on the best practices and standards for data security. The internal IT audit is the function that evaluates the effectiveness and compliance of the data security controls and procedures.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Roles and Responsibilities, Subsection: Data Owner, Page 23.

Question: 563

Which of the following is the PRIMARY reason to regularly update business continuity and disaster recovery documents?

A. To enforce security policy requirements
B. To maintain business asset inventories
C. To ensure audit and compliance requirements are met
D. To ensure the availability of business operations

Answer: D

Explanation:

The primary reason to regularly update business continuity and disaster recovery documents is to ensure that the plans and procedures are aligned with the current business needs and objectives, and that they can effectively support the availability of business operations in the event of a disaster. Updating the documents also helps to enforce security policy requirements, maintain business asset inventories, and ensure audit and compliance requirements are met, but these are secondary benefits.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Business Continuity Planning, Subsection: Business Continuity Plan Maintenance, Page 378.

Question: 564

The PRIMARY reason for creating a business case when proposing an information security project is to:

A. articulate inherent risks.
B. provide demonstrated return on investment (ROI).
C. establish the value of the project in relation to business objectives.
D. gain key business stakeholder engagement.

Answer: C

Explanation:

The primary reason for creating a business case when proposing an information security project is to establish the value of the project in relation to the business objectives and to justify the investment required. A business case should demonstrate how the project aligns with the organization's strategy, goals, and mission, and how it supports the business processes and functions. A business case should also include the expected benefits, costs, risks, and alternatives of the project, and provide a clear rationale for choosing the preferred option.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

Question: 565

Which of the following BEST helps to ensure the effective execution of an organization's disaster recovery plan (DRP)?

A. The plan is reviewed by senior and IT operational management.

B. The plan is based on industry best practices.

C. Process steps are documented by the disaster recovery team.

D. Procedures are available at the primary and failover location.

Answer: D

Explanation:

The best way to ensure the effective execution of a disaster recovery plan (DRP) is to make sure that the procedures are available at both the primary and the failover location, so that the staff can access them in case of a disaster. The procedures should be clear, concise, and updated regularly to reflect the current situation and requirements. Having the procedures available at both locations also helps to avoid confusion and delays in the recovery process.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Recovery Plan Development, Page 373.

Question: 566

The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:

A.)the information security officer.

B. the steering committee.

C. the board of directors.

D. the internal audit manager.

Answer: C

Explanation:

The ultimate responsibility for ensuring the objectives of an information security framework are being met belongs to the board of directors, as they are accountable for the governance of the organization and the oversight of the information security strategy. The board of directors should ensure that the information security framework aligns with the business objectives, supports the business processes, and complies with the legal and regulatory requirements. The board of directors should also monitor the performance and

effectiveness of the information security framework and provide guidance and direction for its improvement.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Enterprise Governance, Subsection: Board of Directors, Page 18.

Question: 567

A newly appointed information security manager has been asked to update all security-related policies and procedures that have been static for five years or more. What should be done NEXT?

A. Update in accordance with the best business practices.
B. Perform a risk assessment of the current IT environment.
C. Gain an understanding of the current business direction.
D. Inventory and review current security policies.

Answer: D

Explanation:

The next step for the information security manager should be to inventory and review the current security policies to understand the existing security requirements, controls, and gaps. This will help to identify the areas that need to be updated, revised, or replaced to align with the current business needs and objectives, as well as the legal and regulatory requirements. Updating the policies in accordance with the best business practices, performing a risk assessment of the current IT environment, or gaining an understanding of the current business direction are important activities, but they should be done after reviewing the current security policies.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Policies, Standards, Procedures and Guidelines, Subsection: Information Security Policies, Page 28.

Question: 568

A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

A. Right of the subscriber to conduct onsite audits of the vendor
B. Escrow of software code with conditions for code release
C. Authority of the subscriber to approve access to its data
D. Commingling of subscribers' data on the same physical server

Answer: C

Explanation:

The greatest concern to an information security manager if omitted from the contract with a multinational cloud computing vendor would be the authority of the subscriber to approve access to its data. This is because the subscriber's data may be subject to different legal and regulatory requirements in different jurisdictions, and the subscriber may lose control over who can access,

process, or disclose its data. The subscriber should have the right to approve or deny access to its data by the vendor or any third parties, and to ensure that the vendor complies with the applicable data protection laws and standards. The authority of the subscriber to approve access to its data is also one of the key elements of the ISACA Cloud Computing Management Audit/Assurance Program1.

Reference = CISM Review Manual, 16th Edition eBook2, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 142.

Question: 569

Which of the following is MOST important when designing security controls for new cloud-based services?

A. Evaluating different types of deployment models according to the associated risks
B. Understanding the business and IT strategy for moving resources to the cloud
C. Defining an incident response policy to protect data moving between onsite and cloud applications
D. Performing a business impact analysis (BIA) to gather information needed to develop recovery strategies

Answer: B

Explanation:

The most important factor when designing security controls for new cloud-based services is to understand the business and IT strategy for moving resources to the cloud. This will help to align the security controls with the business objectives, requirements, and risks, and to select the appropriate cloud service delivery and deployment models. The security controls should also be based on the shared responsibility model, which defines the roles and responsibilities of the cloud service provider and the cloud customer in ensuring the security of the cloud environment. Evaluating different types of deployment models, defining an incident response policy, and performing a business impact analysis are also important activities, but they should be done after understanding the business and IT strategy.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 141-142.

Question: 570

A KEY consideration in the use of quantitative risk analysis is that it:

A. aligns with best practice for risk analysis of information assets.
B. assigns numeric values to exposures of information assets.

C. applies commonly used labels to information assets.
D. is based on criticality analysis of information assets.

Answer: B

Explanation:

A key consideration in the use of quantitative risk analysis is that it assigns numeric values to exposures of information assets, such as the probability of occurrence, the frequency of occurrence, the impact of occurrence, and the monetary value of the assets. These numeric values help to measure and compare the risks in a more objective and consistent way, and to support the decisionmaking process based on cost-benefit analysis. Quantitative risk analysis also requires reliable and accurate data sources, and it may involve the use of statistical tools and techniques.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Analysis, Subsection: Quantitative Risk Analysis, Page 84.

Question: 571

An organization's information security team presented the risk register at a recent information security steering committee meeting. Which of the following should be of MOST concern to the committee?

A. No owners were identified for some risks.
B. Business applications had the highest number of risks.
C. Risk mitigation action plans had no timelines.
D. Risk mitigation action plan milestones were delayed.

Answer: A

Explanation:

The most concerning issue for the information security steering committee should be that no owners were identified for some risks in the risk register. This means that there is no clear accountability and responsibility for managing and mitigating those risks, and that the risks may not be properly addressed or monitored. The risk owners are the persons who have the authority and ability to implement the risk treatment options and to accept the residual risk. The risk owners should be identified and assigned for each risk in the risk register, and they should report the status and progress of the risk management activities to the information security steering committee.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Management, Subsection: Risk Register, Page 104.

Question: 572

Which of the following BEST illustrates residual risk within an organization?

A. Heat map
B. Risk management framework
C. Business impact analysis (BIA)
D. Balanced scorecard

Answer: A

Explanation:

Question: 573

After the occurrence of a major information security incident, which of the following will BEST help an information security manager determine corrective actions?

A. Calculating cost of the incident
B. Conducting a postmortem assessment
C. Performing an impact analysis
D. Preserving the evidence

Answer: B

Explanation:

The best way to determine corrective actions after a major information security incident is to conduct a postmortem assessment, which is a systematic and structured review of the incident, its causes, its impacts, and its lessons learned. A postmortem assessment can help to identify the root causes of the incident, the strengths and weaknesses of the incident response process, the gaps and deficiencies in the security controls, and the opportunities for improvement and remediation. A postmortem assessment can also help to document the recommendations and action plans for preventing or minimizing the recurrence of similar incidents in the future.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 4: Information Security Incident Management, Section: Incident Response, Subsection: Postincident Activities, Page 211.

Question: 574

Before approving the implementation of a new security solution, senior management requires a business case. Which of the following would BEST support the justification for investment?

A. The solution contributes to business strategy.
B. The solution improves business risk tolerance levels.
C. The solution improves business resiliency.
D. The solution reduces the cost of noncompliance with regulations.

Answer: A

Explanation:

The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.

Reference = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

Question: 575

The PRIMARY objective of timely declaration of a disaster is to:

A. ensure engagement of business management in the recovery process.
B. assess and correct disaster recovery process deficiencies.
C. protect critical physical assets from further loss.
D. ensure the continuity of the organization's essential services.

Answer: D

Explanation:

The primary objective of timely declaration of a disaster is to ensure the continuity of the organization’s essential services, which are the services that are critical for the survival and operation of the organization, and that cannot be interrupted or delayed without causing severe consequences. By declaring a disaster, the organization can activate its disaster recovery plan (DRP), which is a set of documented procedures and resources to recover the essential services in the event of a disaster. The DRP should include the roles and responsibilities, the communication channels, the recovery strategies, the backup and restoration procedures, and the testing and maintenance activities for the disaster recovery process1.

Reference = CISM Review Manual, 16th Edition eBook2, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Declaration, Page 372.

Question: 576

What should an information security manager verify FIRST when reviewing an information asset management program?

A. System owners have been identified.
B. Key applications have been secured.
C. Information assets have been classified.

D. Information assets have been inventoried.

Answer: C

Explanation:

According to the CISM Review Manual, information asset classification is the first step in an information asset management program, as it provides the basis for determining the level of protection required for each asset. System owners, key applications and information asset inventory are subsequent steps that depend on the classification of the assets.
Reference = CISM Review Manual, 27th Edition, Chapter 1, Section 1.4.2, page 381.

Question: 577

Company A, a cloud service provider, is in the process of acquiring Company B to gain new benefits by incorporating their technologies within its cloud services.
Which of the following should be the PRIMARY focus of Company A's information security manager?

A. The organizational structure of Company B
B. The cost to align to Company A's security policies
C. Company A's security architecture
D. Company B's security policies

Answer: D

Explanation:

According to the CISM Review Manual, the security architecture of an organization defines the security principles, standards, guidelines and procedures that support the information security strategy and align with the business objectives. When acquiring another company, the information security manager of the acquiring company should focus on ensuring that the security architecture of the acquired company is compatible with its own, or that any gaps or conflicts are identified and resolved.
Reference = CISM Review Manual, 27th Edition, Chapter 2, Section 2.1.2, page 751.

Question: 578

An organization learns that a third party has outsourced critical functions to another external provider. Which of the following is the information security manager's MOST important course of action?

A. Engage an independent audit of the third party's external provider.
B. Recommend canceling the contract with the third party.
C. Evaluate the third party's agreements with its external provider.
D. Conduct an external audit of the contracted third party.

Answer: C

Explanation:

According to the CISM Review Manual, the information security manager should evaluate the third party's agreements with its external provider to ensure that the security requirements and controls are adequate and consistent with the organization's expectations. Engaging or conducting an audit may be a subsequent step, but not the most important one. Recommending canceling the contract may be premature and impractical.
Reference = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.2, page 1431.

Question: 579

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:

A. perform a risk assessment.
B. review the state of security awareness.
C. review information security policies.
D. perform a gap analysis.

Answer: A

Explanation:

According to the CISM Review Manual, performing a risk assessment is the most important course of action for an information security manager during the due diligence phase of an acquisition, as it helps to identify and evaluate the potential threats, vulnerabilities and impacts that may affect the information assets of the target organization. A risk assessment also provides the basis for performing a gap analysis, reviewing the information security policies and awareness, and developing a remediation plan.
Reference = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.1, page 1411.

Question: 580

Which of the following would be MOST useful when determining the business continuity strategy for a large organization's data center?

A. Stakeholder feedback analysis
B. Business continuity risk analysis
C. Incident root cause analysis
D. Business impact analysis (BIA)

Answer: D

Explanation:

According to the CISM Review Manual, a business impact analysis (BIA) is the most useful tool when determining the business continuity strategy for a large organization's data center, as it helps to identify and prioritize the critical business processes and resources that depend on the data center, and the impact of their disruption or loss. A BIA also provides the basis for defining the recovery time objectives (RTOs) and recovery point objectives (RPOs) for the data center, which guide the selection of the appropriate business continuity strategy.
Reference = CISM Review Manual, 27th Edition, Chapter 3, Section 3.5.2, page 1511.

Question: 581

Which of the following is MOST important to include in an information security status report to senior management?

A. Key risk indicators (KRIs)
B. Review of information security policies
C. Information security budget requests
D. List of recent security events

Answer: A

Explanation:

According to the CISM Review Manual, key risk indicators (KRIs) are the most important information to include in an information security status report to senior management, as they provide a measure of the current level of risk exposure and the effectiveness of the risk management activities. KRIs also help to identify trends, patterns and emerging risks that may require management attention or action.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 209

Question: 582

Which of the following should an information security manager do FIRST when a vulnerability has been disclosed?

A. Perform a patch update.
B. Conduct a risk assessment.
C. Perform a penetration test.
D. Conduct an impact assessment.

Answer: B

Explanation:

According to the CISM Review Manual, the first step an information security manager should take when a vulnerability has been disclosed is to conduct a risk assessment to determine the likelihood and impact of the vulnerability being exploited, and the appropriate response strategy. Performing a patch update, a penetration test or an impact assessment are possible subsequent steps, but not the first one.
Reference = CISM Review Manual, 27th Edition, Chapter 3, Section 3.3.2, page 1331.

Question: 583

To prepare for a third-party forensics investigation following an incident involving malware, the incident response team should:

A. isolate the infected systems.
B. preserve the evidence.
C. image the infected systems.
D. clean the malware.

Answer: B

Explanation:

According to the CISM Review Manual, the incident response team should preserve the evidence as the first step to prepare for a third-party forensics investigation, as it helps to maintain the integrity and admissibility of the evidence in a court of law. Preserving the evidence may include isolating and imaging the infected systems, but these are not the only actions required. Cleaning the malware may destroy or alter the evidence and should be avoided until the investigation is completed.
Reference = CISM Review Manual, 27th Edition, Chapter 3, Section 3.6.2, page 165

Question: 584

Which of the following is the MOST important benefit of using a cloud access security broker when migrating to a cloud environment?

A. Enhanced data governance
B. Increased third-party assurance
C.)Improved incident management
D. Reduced total cost of ownership (TCO)

Answer: A

Explanation:

According to the web search results, a cloud access security broker (CASB) is a software solution that stands between the cloud service provider and the cloud service user to enforce security controls. One of the most important benefits of using a CASB when migrating to a cloud environment is enhanced data governance, as it helps to protect sensitive information from unauthorized access, sharing, or loss. A CASB can also provide data classification, encryption, data loss prevention (DLP), and other features that enable organizations to manage and secure their data in the cloud. Reference = What Is a Cloud Access Security Broker (CASB)?, A beginner's guide to cloud access security brokers

Question: 585

Which of the following is the MOST effective defense against malicious insiders compromising confidential information?

A. Regular audits of access controls
B. Strong background checks when hiring staff
C. Prompt termination procedures
D. Role-based access control (RBAC)

Answer: D

Explanation:

role-based access control (RBAC) is the most effective defense against malicious insiders compromising confidential information, as it helps to limit the access of users to the information and resources that are necessary for their roles and responsibilities. RBAC also helps to enforce the principle of least privilege, which reduces the risk of unauthorized or inappropriate access, disclosure, modification, or destruction of information by insiders. RBAC also facilitates the monitoring and auditing of user activities and access rights.
Reference = Malicious insiders | Cyber.gov.au, Insider Threat Mitigation Guide - CISA, Malicious

Insiders: Types, Indicators & Common Techniques - Ekran System

Question: 586

Which of the following BEST enables an organization to identify and contain security incidents?

A. Risk assessments
B. Threat modeling
C. Continuous monitoring
D. Tabletop exercises

Answer: C

Explanation:

= Continuous monitoring is the process of collecting, analyzing, and reporting on the security status of an organization's information systems and networks. Continuous monitoring enables an organization to identify and contain security incidents by providing timely and accurate information on the security events, alerts, incidents, and threats that may affect the organization. Continuous monitoring also helps to measure the effectiveness and compliance of the security controls, policies, and procedures that are implemented to protect the organization's information assets. Continuous monitoring can be performed using various tools and methods, such as security information and event management (SIEM) tools, intrusion detection and prevention systems (IDS/IPS), vulnerability scanners, log analyzers, and audit trails.

Reference = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.2: Continuous Monitoring2

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 3

Question: 587

Communicating which of the following would be MOST helpful to gain senior management support for risk treatment options?

A. Quantitative loss
B. Industry benchmarks
C. Threat analysis
D. Root cause analysis

Answer: A

Explanation:

communicating the quantitative loss associated with the risk scenarios and the risk treatment options would be the most helpful to gain senior management support, as it helps to demonstrate the value and effectiveness of the risk treatment options in terms of reducing the likelihood and impact of the risk. Quantitative loss also helps to compare the cost and benefit of the risk treatment options and to prioritize the most critical risks. Industry benchmarks, threat analysis, and root cause analysis may be useful for understanding and assessing the risk, but they do not directly measure the performance of the risk treatment options.

Reference = Five Key Considerations When Developing Information Security Risk Treatment Plans, CISM Domain 2: Information Risk Management (IRM) [2022 update]

Question: 588

Which of the following should be the PRIMARY objective when establishing a new information security program?

A. Executing the security strategy
B. Minimizing organizational risk
C. Optimizing resources
D. Facilitating operational security

Answer: A

Explanation:

According to the CISM Review Manual, the primary objective when establishing a new information security program is to execute the security strategy that has been defined and approved by the senior management. The security strategy provides the direction, scope, and goals for the information security program, and aligns with the business objectives and requirements. Minimizing organizational risk, optimizing resources, and facilitating operational security are possible outcomes or benefits of the information security program, but they are not the primary objective.
Reference = CISM Review Manual, 27th Edition, Chapter 3, Section 3.1.1, page 1151.

Question: 589

Which of the following events is MOST likely to require an organization to revisit its information security framework?

A. New services offered by IT
B. Changes to the risk landscape
C. A recent cybersecurity attack
D. A new technology implemented

Answer: B

Explanation:

Changes to the risk landscape are the most likely events to require an organization to revisit its information security framework, because they may affect the organization's risk appetite, risk tolerance, risk profile, and risk treatment strategies. The information security framework should be aligned with the organization's business objectives and risk management approach, and should be reviewed and updated regularly to reflect the changing internal and external environment. Reference =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "The information security framework should be reviewed and updated regularly to ensure that it remains aligned with the enterprise's business objectives and risk management approach and reflects the changing internal and external environment."
CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Changes in the risk landscape may require the enterprise to revisit its risk appetite, risk tolerance, risk profile, and risk treatment strategies."

Question: 590

Which of the following is the MOST essential element of an information security program?

A. Benchmarking the program with global standards for relevance
B. Prioritizing program deliverables based on available resources
C. Involving functional managers in program development
D. Applying project management practices used by the business

Answer: C

Explanation:

Involving functional managers in program development is the most essential element of an information security program, because they are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units. They also provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Functional managers are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 38: "Functional managers should be involved in the development of the information security program to provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives."

Question: 591

Which of the following has the MOST influence on the information security investment process?

A. IT governance framework
B. Information security policy
C. Organizational risk appetite
D. Security key performance indicators (KPIs)

Answer: C

Explanation:

Question: 592

An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?

A. Control owner responses based on a root cause analysis
B. The impact of noncompliance on the organization's risk profile
C. A noncompliance report to initiate remediation activities
D. A business case for transferring the risk

Answer: B

Explanation:

The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps them understand the potential consequences of not adhering to the established controls and the need for corrective actions. Noncompliance may expose the organization to increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 84: "The information security manager should report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 85: "Noncompliance with information security policies, standards, and procedures may result in increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities for the enterprise."

Question: 593

Which of the following would provide the BEST input to a business case for a technical solution to address potential system vulnerabilities?

A. Risk assessment
B. Business impact analysis (BIA)
C. Penetration test results
D. Vulnerability scan results

Answer: A

Explanation:

Risk assessment is the BEST input to a business case for a technical solution to address potential system vulnerabilities, because it helps to identify and prioritize the most critical risks that the solution should mitigate or reduce. Risk assessment also helps to evaluate the costs and benefits of the solution in terms of reducing the likelihood and impact of potential threats and incidents. Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 47: "Risk assessment is the process of identifying and analyzing information security risks and determining their potential impact on the enterprise's business objectives."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 48: "Risk assessment provides input to the business case for information security investments by identifying and prioritizing the most critical risks that need to be addressed and evaluating the costs and benefits of the proposed solutions."

Question: 594

To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?

A. Gap analysis results
B. Level of residual risk
C. Level of risk treatment
D. Configuration parameters

Answer: B

Explanation:

Level of residual risk is the amount of risk that remains after applying risk treatment options, such as avoidance, mitigation, transfer, or acceptance. The information security manager should compare the level of residual risk with the organization's risk appetite, which is the amount of risk that the organization is willing to accept in pursuit of its objectives. The comparison will help to determine whether the risk treatment options are sufficient, excessive, or inadequate, and whether further actions are needed to align the risk level with the risk appetite.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 49: "Residual risk is the risk that remains after risk treatment."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 43: "Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in pursuit of value."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "The information security manager should compare the residual risk with the risk appetite and determine whether the risk treatment options are sufficient, excessive, or inadequate."

Question: 595

Which of the following is the BEST way to obtain organization-wide support for an information security program?

A. Mandate regular security awareness training.
B. Develop security performance metrics.
C. Position security as a business enabler.
D. Prioritize security initiatives based on IT strategy.

Answer: C

Explanation:

Positioning security as a business enabler is the BEST way to obtain organization-wide support for an information security program, because it helps to demonstrate the value and benefits of security to the organization's strategic objectives, performance, and reputation. By aligning security with the business goals and needs, the information security manager can gain the buy-in and commitment of senior management and other stakeholders, and foster a positive security culture across the organization.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "The information security manager should position information security as a business enabler that supports the achievement of the enterprise's business objectives and adds value to the enterprise."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 39: "The information security manager should communicate the value and benefits of information security to senior management and other stakeholders to obtain their support and commitment for the information security program." CISM Review Manual, 16th Edition, ISACA, 2020, p. 40: "The information security manager should promote a positive security culture within the enterprise by influencing the behavior and attitude of employees and other parties toward information security."

Question: 596

Which of the following BEST facilitates the development of a comprehensive information security policy?

A. Alignment with an established information security framework
B. An established internal audit program
C. Security key performance indicators (KPIs)
D. Areview of recent information security incidents

Answer: A

Explanation:

Alignment with an established information security framework is the BEST way to facilitate the development of a comprehensive information security policy, because it provides a consistent and structured approach to define, implement, and maintain the policy across the organization. An information security framework is a set of best practices, standards, and guidelines that help to ensure the effectiveness, efficiency, and compliance of the information security policy. Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "An information security framework is a set of best practices, standards, and guidelines that provide a consistent and structured approach to information security governance."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "The information security policy should be aligned with an established information security framework to ensure its effectiveness, efficiency, and compliance."

Question: 597

Which of the following is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider?

A. Obtain an independent audit report.
B. Require the provider to follow stringent data classification procedures.
C. Include high penalties for security breaches in the contract.
D. Review the provider's information security policies.

Answer: B

Explanation:

Requiring the provider to follow stringent data classification procedures is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider, because it helps to define the sensitivity and confidentiality levels of the data and the corresponding security controls and access policies that should be applied. Data classification procedures can help to prevent unauthorized access, disclosure, modification, or deletion of the data, as well as to segregate the data from other customers' data.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Data classification is the process of assigning a level of sensitivity to data that reflects its importance and the impact of its disclosure, alteration, or destruction."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Data classification should be based on the business requirements for confidentiality, integrity, and availability of the data, and should consider the legal, regulatory, and contractual obligations of the enterprise."

Best Practices to Manage Risks in the Cloud - ISACA: "Commingling of data: A big concern many enterprises have with public cloud services is the commingling of data with that of the cloud provider's other customers. One of your first questions should be: "How do you ensure that my data is not commingled with others?" How does the cloud provider ensure that only your team has access to your data?"

Question: 598

An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:

A. the security organization structure.
B. international security standards.
C. risk assessment results.
D. the most stringent requirements.

Answer: C

Explanation:

Question: 599

When developing an information security strategy for an organization, which of the following is MOST helpful for understanding where to focus efforts?

A. Gap analysis
B. Project plans
C. Vulnerability assessment

D. Business impact analysis (BIA)

Answer: A

Explanation:

Gap analysis is the MOST helpful tool for understanding where to focus efforts when developing an information security strategy for an organization, because it helps to identify the current state and the desired state of the information security governance, and the gaps between them. Gap analysis

also helps to prioritize the actions and resources needed to close the gaps and achieve the information security objectives.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Gap analysis is the process of comparing the current state and the desired state of information security governance and identifying the gaps that need to be addressed."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Gap analysis should be performed periodically to assess the effectiveness and efficiency of the information security strategy and program and to identify the areas for improvement."

CISM domain 1: Information security governance [Updated 2022] - Infosec Resources: "Gap analysis: This is a comparison of the current state of security with the desired state. It helps to identify the gaps in security and prioritize the actions required to close them."

Question: 600

Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?

A. Available annual budget
B. Cost-benefit analysis of mitigating controls
C. Recovery time objective (RTO)
D. Maximum tolerable outage (MTO)

Answer: B

Explanation:

Cost-benefit analysis of mitigating controls is the BEST way to assist in determining whether to accept residual risk of a critical security system, because it helps to compare the costs of implementing and maintaining the controls with the benefits of reducing the risk and the potential losses. Cost-benefit analysis can help to justify the investment in security controls and to optimize the level of residual risk that is acceptable for the organization. Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "Cost-benefit analysis is the process of comparing the costs of risk treatment options with the benefits of risk reduction and the potential losses from risk

events."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 51: "Cost-benefit analysis can help to justify the investment in information security controls and to optimize the level of residual risk that is acceptable for the enterprise."

CISM Domain 2: Information Risk Management (IRM) [2022 update]: "Cost-benefit analysis: This is a comparison of the costs of implementing and maintaining security controls with the benefits of reducing risk and potential losses. It helps to justify the investment in security controls and optimize the level of residual risk."

Question: 601

Which of the following is the BEST control to protect customer personal information that is stored in the cloud?

A. Timely deletion of digital records
B. Appropriate data anonymization
C. Strong encryption methods
D. Strong physical access controls

Answer: C

Explanation:

Strong encryption methods are the BEST control to protect customer personal information that is stored in the cloud, because they help to prevent unauthorized access, disclosure, modification, or deletion of the data by encrypting it at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data. Encryption can help to protect the confidentiality, integrity, and availability of the data, as well as to comply with legal and regulatory requirements. Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Encryption is the process of transforming data into an unreadable format using a secret key or algorithm."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Encryption can help to protect the confidentiality, integrity, and availability of data, as well as to comply with legal and regulatory requirements for data protection."

Saas Data Security: Protecting Your Customers' Information In The Cloud - Fresent's Blog: "Encryption and Data Protection: One of the most effective ways to protect sensitive data in the cloud is to encrypt it both at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data."

Question: 602

An organization is experiencing a sharp increase in incidents related to phishing messages. The root cause is an outdated email filtering system that is no longer supported by the vendor. Which of the following should be the information security manager's FIRST course of action?

A. Reinforce security awareness practices for end users.
B. Temporarily outsource the email system to a cloud provider.
C. Develop a business case to replace the system.
D. Monitor outgoing traffic on the firewall.

Answer: C

Explanation:

Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics."

Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages."

Cloud-based email phishing attack using machine and deep learning …: "This attack is used to attack your email account and hack sensitive data easily."

Question: 603

Which of the following should an information security manager do FIRST to address the risk associated with a new third-party cloud application that will not meet organizational security requirements?

A. Include security requirements in the contract.
B. Update the risk register.
C. Consult with the business owner.
D. Restrict application network access temporarily.

Answer: C

Explanation:

Consulting with the business owner is the FIRST course of action that the information security manager should take to address the risk associated with a new third-party cloud application that will not meet organizational security requirements, because it helps to understand the business needs and expectations for using the application, and to communicate the security risks and implications. The information security manager and the business owner should work together to evaluate the trade-offs between the benefits and the risks of the application, and to determine the best course of action, such as modifying the requirements, finding an

alternative solution, or accepting the risk. Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 41: “The information security manager should consult with the business owners to understand their needs and expectations for using third-party services, and to communicate the security risks and implications.”

CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: “The information security manager and the business owners should collaborate to evaluate the trade-offs between the benefits and the risks of using third-party services, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk.”

Best Practices to Manage Risks in the Cloud - ISACA: “The information security manager should work with the business owner to define the security requirements for the cloud service, such as data protection, access control, incident response, and compliance.”

Question: 604

Which of the following is the PRIMARY purpose of an acceptable use policy?

A. To provide steps for carrying out security-related procedures
B. To facilitate enforcement of security process workflows
C. To protect the organization from misuse of information assets
D. To provide minimum security baselines for information assets

Answer: C

Explanation:

The PRIMARY purpose of an acceptable use policy is to protect the organization from misuse of information assets, such as data, hardware, software, and network resources, by defining the rules and expectations for the authorized and appropriate use of these assets by the users. An acceptable use policy helps to prevent or reduce the risks of security breaches, legal liabilities, reputational damage, or loss of productivity that may result from unauthorized, inappropriate, or unethical use of information assets.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 74: “An acceptable use policy is a policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet.”

The essentials of an acceptable use policy - Infosec Resources: “An Acceptable Use Policy (henceforward mentioned as "AUP") is agreement between two or more parties to a computer network community, expressing in writing their intent to adhere to certain standards of behaviour with respect to the proper usage of specific hardware & software services.”

Acceptable use policy template - Workable: “This Acceptable Use Policy sets the minimum requirements for the use of our company’s IT resources, including computers, networks, devices, software, and internet. It aims to protect our company and our employees from harm and liability, and to ensure that our IT resources are used appropriately, productively, and securely.”

Question: 605

Which of the following metrics BEST demonstrates the effectiveness of an organization's security awareness program?

A. Number of security incidents reported to the help desk
B. Percentage of employees who regularly attend security training
C. Percentage of employee computers and devices infected with malware
D. Number of phishing emails viewed by end users

Answer: B

Explanation:

Question: 606

During which phase of an incident response plan is the root cause determined?

A. Recovery
B. Lessons learned
C. Containment
D. Eradication

Answer: D

Explanation:

The eradication phase of an incident response plan is where the root cause of the incident is determined and eliminated. This phase involves identifying and removing all traces of the malicious activity from the affected systems and restoring them to a secure state.
Reference = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

Question: 607

Which of the following BEST helps to enable the desired information security culture within an organization?

A. Information security awareness training and campaigns
B. Effective information security policies and procedures
C. Delegation of information security roles and responsibilities
D. Incentives for appropriate information security-related behavior

Answer: A

Explanation:

Information security awareness training and campaigns are the best way to enable the desired information security culture within an organization because they help to educate, motivate and influence the behavior and attitude of the employees towards information security. They also help to raise the awareness of the risks, threats and best practices of information security among the staff and stakeholders.
Reference = Organizational Culture for Information Security: A Systemic Perspective on the Articulation of Human, Cultural and Social Systems, CISM Exam Content Outline

Question: 608

Which of the following is MOST appropriate to communicate to senior management regarding information risk?

A. Emerging security technologies
B. Risk profile changes
C. Defined risk appetite
D. Vulnerability scanning progress

Answer: B

Explanation:

Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed. Reference = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2: Information Risk Management (IRM) [2022 update]

Question: 609

Which of the following is the BEST way to determine the gap between the present and desired state of an information security program?

A. Perform a risk analysis for critical applications.
B. Determine whether critical success factors (CSFs) have been defined.
C. Conduct a capability maturity model evaluation.
D. Review and update current operational procedures.

Answer: C

Explanation:

A capability maturity model evaluation is the best way to determine the gap between the present and desired state of an information security program because it provides a systematic and structured approach to assess the current level of maturity of the information security processes and practices, and compare them with the desired or target level of maturity that is aligned with the business objectives and requirements. A capability maturity model evaluation can also help to identify the strengths and weaknesses of the information security program, prioritize the improvement areas, and develop a roadmap for achieving the desired state.
Reference = Information Security Architecture: Gap Assessment and Prioritization, CISM Review Manual 15th Edition

Question: 610

Which of the following should be the FIRST step when performing triage of a malware incident?

A. Containing the affected system
B. Preserving the forensic image
C. Comparing backup against production
D. Removing the malware

Answer: A

Explanation:

The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
Reference = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

Question: 611

An information security manager has become aware that a third-party provider is not in compliance with the statement of work (SOW). Which of the following is the BEST course of action?

A. Notify senior management of the issue.
B. Report the issue to legal personnel.
C. Initiate contract renegotiation.
D. Assess the extent of the issue.

Answer: D

Explanation:

The first course of action when the information security manager becomes aware that a third-party provider is not in compliance with the SOW is to assess the extent of the issue, which means determining the nature, scope, and impact of the non-compliance on the security of the enterprise's data and systems. The assessment should also identify the root cause of the non-compliance and the possible remediation actions. The assessment will help the information security manager to decide the next steps, such as notifying senior management, reporting the issue to legal personnel, initiating contract renegotiation, or terminating the contract.
Reference = Ensuring Vendor Compliance and Third-Party Risk Mitigation, A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

Question: 612

Which of the following is the PRIMARY responsibility of the information security function when an organization adopts emerging technologies?

A. Developing security training for the new technologies
B. Designing new security controls
C. Creating an acceptable use policy for the technologies
D. Assessing the potential security risk

Answer: D

Explanation:

The primary responsibility of the information security function when an organization adopts emerging technologies is to assess the potential security risk, which means identifying and evaluating the threats, vulnerabilities, and impacts that the new technologies may pose to the organization's data, systems, and objectives. Assessing the potential security risk helps the information security function to determine the appropriate security requirements, controls, and measures to mitigate the risk and ensure the safe and secure adoption of the emerging technologies. Reference = Performing Risk Assessments of Emerging Technologies, CISM Review Manual 15th Edition

Learn more:

1. isaca.org2. isaca.org3. niccs.cisa.gov4. venturebeat.com 10of30
An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk? A. Requirement for regular information security awareness B. Right-to-audit clause C. Service level agreement (SLA) D. Requirement to comply with corporate security policy Answer: (Refer to the Information Security Manager® (CISM®) documents and learning

Explanation:resources by ISACA available at https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles to verify the answer of the following questions very carefully.) Use the following format please: **Verified Answer** = (From CISM Manual or related resources) **Very Short Explanation** = (From CISM Manual or related resources) **Reference** = (From CISM Manual or related resources)

Question: 613

An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk?

A. Requirement for regular information security awareness
B. Right-to-audit clause
C. Service level agreement (SLA)
D. Requirement to comply with corporate security policy

Answer: D

Explanation:

The most effective way to mitigate information security risk when outsourcing network management to a service provider is to include a requirement for the service provider to comply with the corporate security policy in the contract. This requirement ensures that the service provider follows the same security standards, procedures, and controls as the organization, and protects the confidentiality, integrity, and availability of the organization's data and systems. The requirement also defines the roles and responsibilities, the reporting and escalation mechanisms, and the penalties for non-compliance.
Reference = A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance, CISM Domain 2: Information Risk Management (IRM) [2022 update]

Question: 614

Which of the following is the MOST effective way to convey information security responsibilities across an organization?

A. Implementing security awareness programs
B. Documenting information security responsibilities within job descriptions
C. Developing a skills matrix
D. Defining information security responsibilities in the security policy

Answer: B

Explanation:

Documenting information security responsibilities within job descriptions is the most effective way to convey information security responsibilities across an organization because it clearly defines the roles, expectations, and accountabilities of each employee regarding information security. It also helps to align the information security objectives with the business goals and performance indicators, and to ensure compliance with the security policies and standards.
Reference = CISM Review Manual 15th Edition, What is CISM? - Digital Guardian

Question: 615

An organization wants to integrate information security into its HR management processes. Which of the following should be the FIRST step?

A. Benchmark the processes with best practice to identify gaps.
B. Calculate the return on investment (ROI).
C. Provide security awareness training to HR.
D. Assess the business objectives of the processes.

Answer: D

Explanation:

The first step when integrating information security into HR management processes is to assess the business objectives of the processes, which means understanding the purpose, scope, and expected outcomes of the HR functions and activities, and how they relate to the organization's strategy and goals. The assessment will help to identify the information security requirements, risks, and controls that are relevant and applicable to the HR processes, and to align the information security objectives with the business objectives.
Reference = CISM Review Manual 15th Edition, CISM: Overview of domains [updated 2022]

Question: 616

An organization's automated security monitoring tool generates an excessively large amount of falsq positives. Which of the following is the BEST method to optimize the monitoring process?

A. Report only critical alerts.
B. Change reporting thresholds.
C. Reconfigure log recording.
D. Monitor incidents in a specific time frame.

Answer: B

Explanation:

Changing reporting thresholds is the best method to optimize the monitoring process when the automated security monitoring tool generates an excessively large amount of false positives. Changing reporting thresholds means adjusting the criteria or parameters that trigger the alerts, such as the severity level, the frequency, the source, or the destination of the events. Changing reporting thresholds can help to reduce the number of false positives, filter out the irrelevant or benign events, and focus on the most critical and suspicious events that require further investigation or response.
Reference = Cybersecurity tool sprawl leading to burnout, false positives: report, Security tools' effectiveness hampered by false positives

Question: 617

A project team member notifies the information security manager of a potential security risk that has not been included in the risk register. Which of the following should the information security manager do FIRST?

A. Implement compensating controls.
B. Analyze the identified risk.
C. Prepare a risk mitigation plan.
D. Add the risk to the risk register.

Answer: D

Explanation:

Question: 618

An organization implemented a number of technical and administrative controls to mitigate risk associated with ransomware. Which of the following is MOST important to present to senior management when reporting on the performance of this initiative?

A. The total cost of the investment
B. The cost and associated risk reduction
C. The number and severity of ransomware incidents
D. Benchmarks of industry peers impacted by ransomware

Answer: B

Explanation:

The most important information to present to senior management when reporting on the performance of the initiative to mitigate risk associated with ransomware is the cost and associated risk reduction, which means showing the value and effectiveness of the technical and administrative controls in terms of reducing the likelihood and impact of ransomware incidents and data extortion, and comparing them with the investment and resources required to implement and maintain them. The cost and associated risk reduction can help senior management to evaluate the return on investment (ROI) and the alignment with the business objectives and risk appetite of the initiative. Reference = Ransomware Risk Management - NIST, #StopRansomware Guide | CISA

Question: 619

Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?

A. Inform the public relations officer.
B. Monitor the third party's response.
C. Invoke the incident response plan.
D. Inform customers of the breach.

Answer: C

Explanation:

The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.

Reference = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

Question: 620

A new application has entered the production environment with deficient technical security controls.
Which of the following is MOST Likely the root cause?

A. Inadequate incident response controls
B. Lack of legal review
C. Inadequate change control
D. Lack of quality control

Answer: C

Explanation:

Change control is the process of ensuring that changes to an information system are authorized, tested, documented and implemented in a controlled manner. Inadequate change control can result in deficient technical security controls, such as missing patches, misconfigurations, vulnerabilities or errors in the new application.

Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291

Question: 621

Which of the following is MOST important when developing an information security strategy?

A. Engage stakeholders.
B. Assign data ownership.

C. Determine information types.
D. Classify information assets.

Answer: A

Explanation:

Engaging stakeholders is the most important step when developing an information security strategy, as it ensures that the strategy is aligned with the business objectives, risks, and needs of the organization. Stakeholders include senior management, business units, IT staff, customers, regulators, and other relevant parties who have an interest or influence on the information security of the organization. By engaging stakeholders, the information security manager can gain their support, input, feedback, and buy-in for the strategy, as well as identify and prioritize the security requirements, expectations, and challenges.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 1

Question: 622

Which of the following is MOST important to consider when choosing a shared alternate location for computing facilities?

A. The organization's risk tolerance
B. The organization's mission
C. Resource availability
D. Incident response team training

Answer: A

Explanation:

The organization’s risk tolerance is the most important factor to consider when choosing a shared alternate location for computing facilities, as it determines the acceptable level of risk exposure and the required recovery time objective (RTO) for the organization. A shared alternate location is a facility that is used by multiple organizations for disaster recovery purposes, and it may have limited resources, availability, and security. Therefore, the organization must assess its risk tolerance and ensure that the shared alternate location can meet its recovery requirements and protect its information assets.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291; CISM Online Review Course, Module 4, Lesson 3, Topic 22; BCMpedia, Alternate Site3

Question: 623

An international organization with remote branches is implementing a corporate security policy for managing personally identifiable information (PII). Which of the following should be the information security manager's MAIN concern?

A. Local regulations
B. Data backup strategy
C. Consistency in awareness programs
D. Organizational reporting structure

Answer: A

Explanation:

Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure that the policy complies with the applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

Question: 624

An organization experienced a loss of revenue during a recent disaster. Which of the following would BEST prepare the organization to recover?

A. Business impact analysis (BIA) B. Business continuity plan (BCP) C. Incident response plan D. Disaster recovery plan (DRP)

Answer: B

Explanation:

Question: 625

Which of the following control types should be considered FIRST for aligning employee behavior with an organization's information security objectives?

A. Administrative security controls
B. Technical security controls
C. Physical security controls
D. Access security controls

Answer: A

Explanation:

Question: 626

Which of the following is the BEST course of action when an information security manager identifies that systems are vulnerable to emerging threats?

A. Frequently update systems and monitor the threat landscape.
B. Monitor the network containing the affected systems for malicious traffic.
C. Increase awareness of the threats among employees who work with the systems.
D. Notify senior management and key stakeholders of the threats.

Answer: A

Explanation:

The best course of action when an information security manager identifies that systems are vulnerable to emerging threats is to frequently update systems and monitor the threat landscape, as this will help to reduce the exposure and impact of the threats, and enable timely detection and

response. Updating systems involves applying patches, fixing vulnerabilities, and implementing security controls. Monitoring the threat landscape involves collecting and analyzing threat intelligence, identifying new attack vectors and techniques, and assessing the risk and impact of the threats.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2211; State of Cybersecurity 2023: Navigating Current and Emerging Threats2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

Question: 627

The categorization of incidents is MOST important for evaluating which of the following?

A. Appropriate communication channels
B. Allocation of needed resources
C. Risk severity and incident priority
D. Response and containment requirements

Answer: C

Explanation:

The categorization of incidents is most important for evaluating the risk severity and incident priority, as these factors determine the impact and urgency of the incident, and the appropriate level of response and escalation. The categorization of incidents helps to classify the incidents based on their type, source, cause, scope, and affected assets or services. By categorizing incidents, the information security manager can assess the potential or actual harm to the organization, its stakeholders, and its objectives, and assign a priority level that reflects the need for immediate action and resolution. The risk severity and incident priority also influence

the allocation of resources, the response and containment requirements, and the communication channels, but they are not the primary purpose of categorization.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.4.1, page 2371; CISM Online Review Course, Module 4, Lesson 4, Topic 12; CIRT Case Classification (Draft) - FIRST3

Question: 628

The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:

A. the internal audit manager.
B. the information security officer.
C. the steering committee.
D. the board of directors.

Answer: D

Explanation:

The board of directors is the ultimate authority and accountability for ensuring the objectives of an information security framework are being met, as they are responsible for setting the strategic direction, approving the policies, overseeing the performance, and ensuring the compliance of the organization. The board of directors also delegates the authority and resources to the information security officer, the steering committee, and the internal audit manager, who are involved in the design, implementation, monitoring, and improvement of the information security framework. Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12; CISM domain 1: Information security governance Updated 2022

Question: 629

Which of the following is a PRIMARY responsibility of the information security goxernance function?

A. Administering information security awareness training
B. Defining security strategies to support organizational programs
C. Ensuring adequate support for solutions using emerging technologies
D. Advising senior management on optimal levels of risk appetite and tolerance

Answer: B

Explanation:

Defining security strategies to support organizational programs is a primary responsibility of the information security governance function, as it involves providing strategic direction for security activities and ensuring that objectives are achieved. According to ISACA, information security governance is a subset of corporate

Watermark Sample

governance that provides guidance for aligning information security with business objectives, managing information security risks, and using information resources responsibly12.

Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12

Question: 630

Which of the following is MOST important to include in security incident escalation procedures?

A. Key objectives of the security program
B. Recovery procedures
C. Notification criteria
D. Containment procedures

Answer: C

Explanation:

The most important thing to include in security incident escalation procedures is notification criteria. This is because notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. Notification criteria help to ensure that the appropriate stakeholders are aware of the incident and can take the necessary actions to respond, mitigate, and recover from it. Notification criteria also help to comply with legal and regulatory requirements for reporting incidents to external parties, such as customers, authorities, or media.

Notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. (From CISM Manual or related resources) Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2121; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 1, page 1

Question: 631

Which of the following BEST facilitates recovery of data lost as a result of a cybersecurity incident?

A. Removable storage media
B. Disaster recovery plan (DRP)
C. Offsite data backups
D. Encrypted data drives

Answer: C

Explanation:

The best option to facilitate recovery of data lost as a result of a cybersecurity incident is offsite data backups.

This is because offsite data backups provide a secure and reliable way to restore data that may have been corrupted, deleted, or encrypted by malicious actors. Offsite data backups also reduce the risk of data loss due to physical damage, theft, or natural disasters that may affect the primary data storage location. Offsite data backups should be part of a comprehensive disaster recovery plan (DRP) that defines the roles, responsibilities, procedures, and resources for restoring normal operations after a cyber incident.

Question: 632

Which of the following should have the MOST influence on an organization's response to a new industry regulation?

A. The organization's control objectives
B. The organization's risk management framework
C. The organization's risk appetite
D. The organization's risk control baselines

Answer: C

Explanation:

The most influential factor on an organization’s response to a new industry regulation is the organization’s risk appetite. This is because the risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives, and it guides the decision-making process for managing risks. The risk appetite also determines the extent to which the organization needs to comply with the new regulation, and the resources and actions required to achieve compliance. The risk appetite should be aligned with the organization’s strategy, culture, and values, and it should be communicated and monitored throughout the organization.

Question: 633

An organization is considering using a third party to host sensitive archived dat
a. Which of the following is MOST important to verify before entering into the relationship?

A. The vendor's data centers are in the same geographic region.
B. The encryption keys are not provisled to the vendor.
C. The vendor's controls are in line with the organization's security standards.
D. Independent audits of the vendor's operations are regularly conducted.

Answer: C

Explanation:

The most important thing to verify before entering into a relationship with a third party to host sensitive archived data is the vendor’s controls are in line with the organization’s security standards. This is because the organization is ultimately responsible for the security and privacy of its data, even if it is stored or processed by a third party. The organization should ensure that the vendor has adequate and effective controls to protect

the data from unauthorized access, modification, disclosure, or destruction. The organization should also ensure that the vendor complies with the applicable laws and regulations regarding data protection, such as the General Data Protection Regulation (GDPR) in the European Union. The organization should conduct a thorough risk assessment of the vendor and its services, and establish a clear contract that defines the roles, responsibilities, expectations, and obligations of both parties.
Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 2, page 2

Question: 634

Which of the following BEST indicates that an information security governance framework has been successfully implemented?

A. The framework aligns internal and external resources.
B. The framework aligns security processes with industry best practices.
C. The framework aligns management and other functions within the security organization.
D. The framework includes commercial off-the-shelf security solutions.

Answer: A

Explanation:

The best indicator that an information security governance framework has been successfully implemented is A. The framework aligns internal and external resources. This is because the framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities.
The framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities. (From CISM Manual or related resources) Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 49, page 14

Question: 635

Which of the following is the BEST starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities?

A. Controls analysis
B. Emerging risk review
C. Penetration testing
D. Traffic monitoring

Answer: C

Explanation:

The best starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities is C. Penetration testing. This is because penetration testing is a method of simulating real-world attacks on a network to evaluate its security posture and identify any weaknesses or gaps that could be exploited by malicious actors. Penetration testing can help the information security manager to assess the effectiveness of the existing controls, prioritize the remediation efforts, and demonstrate compliance with the relevant standards and regulations. Penetration testing can also provide valuable insights into the network architecture, configuration, and behavior, as well as the potential impact and likelihood of different types of attacks.

Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 50, page 14

Question: 636

What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?

A. Developing a dashboard for communicating the metrics
B. Agreeing on baseline values for the metrics
C. Benchmarking the expected value of the metrics against industry standards
D. Aligning the metrics with the organizational culture

Answer: D

Explanation:

The most important consideration when establishing metrics for reporting to the information security strategy committee is D. Aligning the metrics with the organizational culture. This is because the metrics should reflect the values, beliefs, and behaviors of the organization and its stakeholders, and support the achievement of the strategic objectives and goals. The metrics should also be relevant, meaningful, and understandable for the intended audience, and provide clear and actionable information for decision making. The metrics should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.

Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 5, page 3

Question: 637

Which of the following BEST enables the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption?

A. Service level agreement (SLA) B. Business continuity plan (BCP) C. Disaster recovery plan (DRP) D. Business impact analysis (BIA)

Answer: B

Explanation:

The best option to enable the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption is B. Business continuity plan (BCP). This is because a BCP is a documented collection of procedures and information that guides the organization to prepare for, respond to, and recover from a disruption, such as a natural disaster, a cyberattack, or a pandemic. A BCP aims to ensure the continuity of the critical business functions and processes that support the delivery of products and services to the customers and stakeholders. A BCP also defines the roles, responsibilities, resources, and actions required to maintain the operational resilience of the organization in the face of a disruption.

Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.3, page 2141; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 6, page 3

Question: 638

An organization is performing due diligence when selecting a third party. Which of the following is MOST helpful to reduce the risk of unauthorized sharing of information during this process?

A. Using secure communication channels
B. Establishing mutual non-disclosure agreements (NDAs)
C. Requiring third-party privacy policies
D. Obtaining industry references

Answer: B

Explanation:

The best option to reduce the risk of unauthorized sharing of information during the due diligence process is B. Establishing mutual non-disclosure agreements (NDAs). This is because NDAs are legal contracts that bind the parties to keep confidential any information that is exchanged or disclosed during the due diligence process. NDAs can help to protect the sensitive data, intellectual property, trade secrets, or business strategies of both the organization and the third party from being leaked, stolen, or misused by unauthorized parties. NDAs can also specify the terms and conditions for the use, storage, and disposal of the information, as well as the consequences for breaching the agreement.

Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 70, page 18

Question: 639

Which of the following should be done FIRST when a SIEM flags a potential event?

A. Validate the event is not a false positive.
B. Initiate the incident response plan.
C. Escalate the event to the business owner.
D. Implement compensating controls.

Answer: A

Explanation:

The first thing that should be done when a SIEM flags a potential event is A. Validate the event is not a false positive. This is because a false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. False positives can waste the time and resources of the security team, and reduce the trust and confidence in the SIEM system. Therefore, it is important to verify the accuracy and validity of the event before initiating any further actions, such as incident response, escalation, or compensating controls. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise.
A false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 72, page 19

Question: 640

Which of the following should an information security manager do NEXT after creating a roadmap to execute the strategy for an information security program?

A. Obtain consensus on the strategy from the executive board.
B. Review alignment with business goals.
C. Define organizational risk tolerance.
D. Develop a project plan to implement the strategy.

Answer: D

Explanation:

The next thing that an information security manager should do after creating a roadmap to execute the strategy for an information security program is D. Develop a project plan to implement the strategy. This is

because a project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. A project plan can help the information security manager to organize, coordinate, monitor, and control the activities and resources required to execute the strategy and achieve the desired outcomes. A project plan can also facilitate communication, collaboration, and reporting among the project team, stakeholders, and sponsors.
A project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.2, page 1281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 74, page 19

Question: 641

Which of the following is the MOST effective way to determine the alignment of an information security program with the business strategy?

A. Evaluate the results of business continuity testing.
B. Review key performance indicators (KPIs).
C. Evaluate the business impact of incidents.
D. Engage business process owners.

Answer: D

Explanation:

The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.
Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20

Question: 642

Which of the following is the PRIMARY objective of information asset classification?

A. Vulnerability reduction
B. Compliance management
C. Risk management
D. Threat minimization

Answer: C

Explanation:

The primary objective of information asset classification is C. Risk management. This is because information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. Information asset classification also helps the organization to comply with the legal, regulatory, and contractual obligations regarding the information assets, and to optimize the use of resources and costs for information security.

Information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 7, page 3; Certified Information Security Manager Exam Prep Guide - Packt Subscription2

Question: 643

Which of the following is MOST important to complete during the recovery phase of an incident response process before bringing affected systems back online?

A. Record and close security incident tickets.
B. Test and verify that compromisedsystems are clean.
C. Document recovery steps for senior management reporting.
D. Capture and preserve forensic images of affected systems.

Answer: B

Explanation:

Question: 644

An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

A. To facilitate the continuous improvement of the IT organization

B. To ensure controls align with security needs
C. To create and document required IT capabilities
D. To prioritize security risks on a longer scale than the one-year plan

Answer: B

Explanation:

The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The longterm plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.

The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3: Information security program development and management [2022 update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

Question: 645

Which of the following is MOST important for the improvement of a business continuity plan (BCP)?

A. Incorporating lessons learned
B. Implementing an IT resilience solution
C. Implementing management reviews
D. Documenting critical business processes

Answer: A

Explanation:

Question: 646

Which of the following is the BEST way to help ensure alignment of the information security program with organizational objectives?

A. Establish an information security steering committee.
B. Employ a process-based approach for information asset classification.
C. Utilize an industry-recognized risk management framework.

D. Provide security awareness training to board executives.

Answer: A

Explanation:

The best way to help ensure alignment of the information security program with organizational objectives is A. Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security program is aligned with the organizational objectives by: Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders
Defining and approving the information security policies, standards, and procedures
Establishing and monitoring the information security goals, metrics, and performance indicators Allocating and prioritizing the resources and budget for information security initiatives and projects Resolving any conflicts or issues that may arise between the information security function and the business units
Reviewing and endorsing the information security risk assessment and treatment plans
Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security
An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

Question: 647

When establishing an information security governance framework, it is MOST important for an information security manager to understand:

A. information security best practices.
B. risk management techniques.
C. the threat environment.
D. the corporate culture.

Answer: D

Explanation:

Question: 648

An enterprise has decided to procure security services from a third-party vendor to support its information security program. Which of the following is MOST important to include in the vendor selection criteria?

A. Feedback from the vendor's previous clients
B. Alignment of the vendor's business objectives with enterprise security goals
C. The maturity of the vendor's internal control environment
D. Penetration testing against the vendor's network

Answer: B

Explanation:

The most important thing to include in the vendor selection criteria when procuring security services from a third-party vendor is B. Alignment of the vendor's business objectives with enterprise security goals. This is because the vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. The vendor should also be able to demonstrate how their services add value, reduce risk, and enhance the performance and maturity of the enterprise's information security program. The alignment of the vendor's business objectives with enterprise security goals can help to ensure a successful and long-term partnership, and avoid any conflicts, gaps, or issues that may arise from misalignment or divergence.

The vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; Third-Party Vendor Selection: If Done Right, It's a Win-Win2; Vendor Selection Criteria: Key Factors in Procurement Success3

Question: 649

Which of the following BEST indicates the organizational benefit of an information security solution?

A. Cost savings the solution brings to the information security department
B. Reduced security training requirements
C. Alignment to security threats and risks
D. Costs and benefits of the solution calculated over time

Answer: D

Explanation:

The best option to indicate the organizational benefit of an information security solution is D. Costs and benefits of the solution calculated over time. This is because costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. ROSI can also help to justify the allocation and optimization of the resources and budget for the information security solution, and to compare and prioritize different security alternatives. ROSI can be calculated by using various methods and formulas, such as the annualized loss expectancy (ALE), the annualized rate of occurrence (ARO), and the cost-benefit analysis (CBA).

Costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI),

can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.3, page 1311; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 99, page 26; How to Calculate Return on Security Investment (ROSI) - Infosec2

Question: 650

Which of the following is necessary to ensure consistent protection for an organization's information assets?

A. Classification model
B. Control assessment
C. Data ownership
D. Regulatory requirements

Answer: A

Explanation:

The answer to the question is A. Classification model. This is because a classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by:

Providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets

Enabling the identification and prioritization of the information assets that need the most protection and resources

Facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification

Supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA)

A classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets, enabling the identification and prioritization of the information assets that need the most protection and resources, facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification, and supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISA Domain 5 - Protection of Information Assets2; CISM domain 3: Information security program development and management [2022 update]3; CISM Domain 2: Information Risk Management (IRM) [2022 update]4

Question: 651

Which of the following is the MOST important consideration when developing key performance indicators (KPIs) for the information security program?

A. Alignment with financial reporting
B. Alignment with business initiatives
C. Alignment with industry frameworks
D. Alignment with risk appetite

Answer: B

Explanation:

Explore
The most important consideration when developing key performance indicators (KPIs) for the information security program is B. Alignment with business initiatives. This is because KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and
support the achievement of the desired outcomes and benefits. KPIs should also reflect the needs, expectations, and challenges of the business stakeholders, and provide relevant, meaningful, and actionable information for decision making and improvement. KPIs should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Domain – Information Security Program Development | Infosec2; KPIs in Information Security: The 10 Most Important Security Metrics3

Question: 652

Which of the following should be updated FIRST when aligning the incident response plan with the corporate strategy?

A. Disaster recovery plan (DRP)
B. Incident notification plan
C. Risk response scenarios
D. Security procedures

Answer: C

Explanation:

The answer to the question is C. Risk response scenarios. This is because risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents, such as cyberattacks, natural disasters, or data breaches. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization, and guides the decision-making and resource allocation processes. By aligning the risk response scenarios with the corporate strategy, the organization can ensure that the incident response plan supports the achievement of the desired outcomes and benefits, and minimizes the impact and disruption to the business operations and performance.

Risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2111; CISM domain 4: Information security incident management [2022 update] | Infosec2; A Guide to Effective Incident Management Communications3

Question: 653

Which of the following is the PRIMARY advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program?

A. It offers the organization flexible deployment options using cloud infrastructure.
B. It allows the organization to prioritize its core operations.
C. It is more secure than traditional data backup architecture.
D. It allows the use of a professional response team at a lower cost.

Answer: B

Explanation:

The primary advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program is B. It allows the organization to prioritize its core operations. This is because DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster1. DRaaS can help the organization to prioritize its core operations by: Reducing the need for provisioning and maintaining its own off-site disaster recovery environment, which can be costly, complex, and resource-intensive12 Enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment instead of from the disaster-affected physical servers, which can minimize the downtime, data loss, and business disruption12 Providing the organization with flexible and scalable deployment options, such as on-demand, pay- per-use, or

subscription-based models, that can meet its changing business needs and budget12 Leveraging the expertise, experience, and best practices of the service provider, who can handle the disaster recovery planning, testing, and execution, and ensure compliance with the relevant standards and regulations12
DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster. DRaaS can help the organization to prioritize its core operations by reducing the need for provisioning and maintaining its own off-site disaster recovery environment, enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment, providing the organization with flexible and scalable deployment options, and leveraging the expertise, experience, and best practices of the service provider. (From CISM Manual or related resources)

Question: 654

Which of the following would be MOST effective in reducing the impact of a distributed denial of service (DDoS) attack?

A. Impose state limits on servers.
B. Spread a site across multiple ISPs.
C. Block the attack at the source.
D. Harden network security.

Answer: B

Explanation:

The answer to the question is B. Spread a site across multiple ISPs. This is because spreading a site across multiple Internet service providers (ISPs) can help to reduce the impact of a distributed denial of service (DDoS) attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. Spreading a site across multiple ISPs can also help to distribute the traffic load and balance the performance of the site, and to mitigate the effects of regional or network-specific outages or disruptions. Spreading a site across multiple ISPs can be done by using various techniques, such as anycast routing, content delivery networks (CDNs), or cloud-based services12.
Spreading a site across multiple ISPs can help to reduce the impact of a DDoS attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. (From CISM Manual or related resources)
Reference = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; DDoS Attacks —A Cyberthreat and Possible Solutions2

Question: 655

Which of the following is the GREATEST benefit of incorporating information security governance into the corporate governance framework?

A. Heightened awareness of information security strategies
B. Improved process resiliency in the event of attacks

C. Promotion of security-by-design principles to the business

D. Management accountability for information security

Answer: D

Explanation:

The greatest benefit of incorporating information security governance into the corporate governance framework is D. Management accountability for information security. This is because management accountability for information security means that the senior management and the board of directors are responsible for defining, overseeing, and supporting the information security strategy, policies, and objectives of the organization, and ensuring that they are aligned with the business

goals, stakeholder expectations, and regulatory requirements. Management accountability for information security also means that the senior management and the board of directors are accountable for the performance, value, and effectiveness of the information security program, and for the management and mitigation of the information security risks and incidents. Management accountability for information security can help to foster a culture of security awareness and responsibility, and to enhance the trust and confidence of the customers, partners, and regulators in the organization's information security capabilities. Management accountability for information security means that the senior management and the board of directors are responsible for defining, overseeing, and supporting the information security strategy, policies, and objectives of the organization, and ensuring that they are aligned with the business goals, stakeholder expectations, and regulatory requirements. (From CISM Manual or related resources)

Reference = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM domain 1: Information security governance [Updated 2022] | Infosec2; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition3

Question: 656

Which of the following is the BEST reason to implement a comprehensive information security management system?

To ensure continuous alignment with the organizational strategy

To gain senior management support for the information security program

To support identification of key risk indicators (KRIs)

A. To facilitate compliance with external regulatory requirements

Answer: A

Explanation:

According to the CISM Review Manual, 15th Edition, the primary objective of an information security

management system (ISMS) is to align the information security strategy with the business strategy and ensure that information security objectives are consistent with the business objectives1. This helps the organization to achieve its goals and protect its information assets from threats and risks. Reference = 1: CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, page 11.

Question: 657

Which of the following is the BEST reason for senior management to support a business case for developing a monitoring system for a critical application?

A. An industry peer experienced a recent breach with a similar application.
B. The system can be replicated for additional use cases.
C. The cost of implementing the system is less than the impact of downtime.
D. The solution is within the organization's risk tolerance.

Answer: C

Explanation:

A monitoring system for a critical application can help detect and prevent incidents that could affect the availability, integrity, and confidentiality of the application and its data. The impact of downtime could include loss of revenue, reputation, customer satisfaction, and regulatory compliance.

Therefore, the cost of implementing the system should be justified by the potential savings from avoiding or minimizing these impacts.

Reference = CISM Review Manual, 15th Edition, page 173; An Introduction to Metrics, Monitoring, and Alerting; Business-critical applications: What are they and how do you protect them from cyberattack?

Question: 658

Which of the following roles has the PRIMARY responsibility to ensure the operating effectiveness of IT controls?

A. Risk owner
B. Control tester
C. IT compliance leader
D. Information security manager

Answer: D

Explanation:

According to the CISM Review Manual, 15th Edition1, the information security manager is responsible for ensuring that the information security program supports the organization’s objectives and aligns with applicable laws and regulations. The information security manager is also responsible for overseeing the implementation and maintenance of effective IT controls, as well as monitoring and reporting on their

performance.

Reference = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 1, page 10.

Question: 659

Which of the following should be done NEXT following senior management's decision to comply with new personal data regulations that are much more stringent than those currently followed to avoid

massive fines?

A. Encrypt data in transit and at rest.
B. Complete a return on investment (ROI) analysis.
C. Create and implement a data minimization plan.
D. Conduct a gap analysis.

Answer: D

Explanation:

A gap analysis is a tool that helps to identify the current state of compliance and the desired state of compliance, as well as the actions needed to achieve the desired state. A gap analysis should be done before implementing any specific controls or solutions, such as encryption, data minimization, or ROI analysis.

Reference = CISM Review Manual 15th Edition, page 65; Information Security Architecture: Gap Assessment and Prioritization, ISACA Journal, volume 2, 2018.

Question: 660

Predetermined containment methods to be used in a cybersecurity incident response should be based PRIMARILY on the:

A. number of impacted users.
B. capability of incident handlers.
C. type of confirmed incident.
D. predicted incident duration.

Answer: C

Explanation:

According to the NIST SP 800-61 Computer Security Incident Handling Guide, the type of confirmed incident is one of the most important criteria for choosing a containment strategy, as different types of incidents may require different levels of urgency, scope, and impact1. For example, a denial-of- service attack may require a different containment strategy than a ransomware attack or a data breach.

Reference = 1: NIST SP 800-61: 3.1. Choosing a Containment Strategy2

Question: 661

How would the information security program BEST support the adoption of emerging technologies?

A. Conducting a control assessment
B. Developing an emerging technology roadmap
C. Providing effective risk governance
D. Developing an acceptable use policy

Answer: B

Explanation:

An emerging technology roadmap is a strategic plan that identifies the potential benefits, risks, and challenges of adopting new technologies in alignment with the organization's goals and objectives. It also defines the roles and responsibilities, processes, and controls for managing the technology lifecycle, from evaluation to implementation to maintenance. An emerging technology roadmap can help the information security program support the adoption of emerging technologies by ensuring that security requirements are considered and addressed at every stage, and that the technologies are aligned with the organization's risk appetite and compliance obligations.

Reference = CISM Review Manual, 15th Edition, page 97; Privacy, Security and Bias in Emerging Technologies; The Impact of Emerging Technology on the Future of Cybersecurity

Question: 662

Which of the following BEST determines an information asset's classification?

A. Value of the information asset in the marketplace
B. Criticality to a business process
C. Risk assessment from the data owner
D. Cost of producing the information asset

Answer: B

Explanation:

According to the CISM Review Manual, 15th Edition1, information asset classification is the process of assigning a level of sensitivity to information assets based on their importance to the organization and the potential impact of unauthorized disclosure, modification or destruction. The criticality of an information asset to a business process is one of the key factors that determines its classification level.

Reference = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 2, page 61.

Question: 663

An information security team has confirmed that threat actors are taking advantage of a newly announced critical vulnerability within an application. Which of the following should be done FIRST?

A. Install additional application controls.
B. Notify senior management.
C. Invoke the incident response plan.
D. Prevent access to the application.

Answer: C

Explanation:

According to the NIST SP 800-61 Computer Security Incident Handling Guide1, the first step in responding to a cybersecurity incident is to invoke the incident response plan (IRP), which is a written document that defines the roles, responsibilities, and procedures for dealing with a confirmed or suspected security breach1. The IRP helps the organization to prepare for, detect, analyze, contain, eradicate, recover from, and learn from incidents1. Invoking the IRP ensures that the right personnel and resources are mobilized to effectively deal with the threat and minimize the impact.
Reference = 1: NIST SP 800-61: 1. Introduction1

Question: 664

Which of the following is the MOST effective way to increase security awareness in an organization?

A. Implement regularly scheduled information security audits.
B. Require signed acknowledgment of information security policies.
C. Conduct periodic simulated phishing exercises.
D. Include information security requirements in job descriptions.

Answer: C

Explanation:

Question: 665

The results of a risk assessment for a potential network reconfiguration reveal a high likelihood of sensitive data being compromised. What is the information security manager's BEST course of action?

A. Recommend additional network segmentation.
B. Seek an independent opinion to confirm the findings.
C. Determine alignment with existing regulations.
D. Report findings to key stakeholders.

Answer: D

Explanation:

The information security manager's best course of action is to report the findings of the risk assessment to the key stakeholders, such as senior management, business owners, and regulators. This will ensure that the stakeholders are aware of the potential impact of the risk and can make informed decisions on how to address it. The other options are possible actions to take after reporting the findings, but they are not the best course of action in this scenario.

Reference = CISM Domain 2: Information Risk Management (IRM) [2022 update] (section: Information Risk Response) and CISM ITEM DEVELOPMENT GUIDE - ISACA (page 6, item example 2)

Question: 666

Which of the following is an information security manager's BEST course of action when a penetration test reveals a security exposure due to a firewall that is not configured correctly?

A. Ensure a plan with milestones is developed.
B. Implement a distributed denial of service (DDoS) control.
C. Engage the incident response team.
D. Define new key performance indicators (KPIs).

Answer: A

Explanation:

A penetration test is a proactive way to identify and remediate security vulnerabilities in a network. When a penetration test reveals a security exposure due to a firewall that is not configured correctly, the information security manager's best course of action is to ensure a plan with milestones is developed to address the issue. This plan should include the root cause analysis, the corrective actions, the responsible parties, the deadlines, and the verification methods. This way, the information security manager can ensure that the security exposure is resolved in a timely and effective manner, and that the firewall configuration is aligned with the security policy and the business objectives.

Reference =

CISM Review Manual (Digital Version), page 193: "The information security manager should ensure that a plan with milestones is developed to address the issues identified during the penetration test."

How to configure a network firewall: Walkthrough: "A good network firewall is essential. Learn the basics of configuring a network firewall, including stateful vs. stateless firewalls and access control lists in this episode of Cyber Work Applied."

Which of the following is the BEST way to evaluate whether the information security program aligns with corporate governance?

A . Survey mid-level management.

B . Analyze industry benchmarks.

C . Conduct a gap analysis.

D . Review internal audit reports.

Question: 667

Which of the following is the MOST important objective when planning an incident response program?

A. Managing resources
B. Ensuring IT resiliency
C. Recovering from a disaster
D. Minimizing business impact

Answer: D

Explanation:

Question: 668

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

A. relates the investment to the organization's strategic plan.
B. translates information security policies and standards into business requirements.
C. articulates management's intent and information security directives in clear language.
D. realigns information security objectives to organizational strategy.

Answer: D

Explanation:

Question: 669

Which of the following presents the GREATEST challenge to a large multinational organization using an automated identity and access management (1AM) system?

A. Staff turnover rates that significantly exceed industry averages
B. Large number of applications in the organization

C. Inaccurate workforce data from human resources (HR)
D. Frequent changes to user roles during employment

Answer: C

Explanation:

Question: 670

When an organization lacks internal expertise to conduct highly technical forensics investigations, what is the BEST way to ensure effective and timely investigations following an information security incident?

A. Purchase forensic standard operating procedures.
B. Provide forensics training to the information security team.
C. Ensure the incident response policy allows hiring a forensics firm.
D. Retain a forensics firm prior to experiencing an incident.

Answer: C

Explanation:

Question: 671

Which of the following considerations is MOST important when selecting a third-party intrusion detection system (IDS) vendor?

A. The vendor's proposal allows for contract modification during technology refresh cycles.
B. The vendor's proposal aligns with the objectives of the organization.
C. The vendor's proposal requires the provider to have a business continuity plan (BCP).
D. The vendor's proposal allows for escrow in the event the third party goes out of business.

Answer: B

Explanation:

Question: 672

A software vendor has announced a zero-day vulnerability that exposes an organization's critical business systems. The vendor has released an emergency patch. Which of the following should be the information security managers PRIMARY concern?

A. Ability to test the patch prior to deployment
B. Documentation of patching procedures
C. Adequacy of the incident response plan
D. Availability of resources to implement controls

Answer: D

Explanation:

Question: 673

A new information security manager finds that the organization tends to use short-term solutions to address problems. Resource allocation and spending are not effectively tracked, and there is no assurance that compliance requirements are being met. What should be done FIRST to reverse this bottom-up approach to security?

A. Conduct a threat analysis.
B. Implement an information security awareness training program.
C. Establish an audit committee.
D. Create an information security steering committee.

Answer: D

Explanation:

Question: 674

Of the following, who is BEST suited to own the risk discovered in an application?

A. Information security manager
B. Senior management
C. System owner
D. Control owner

Answer: C

Explanation:

Question: 675

A business unit recently integrated the organization's new strong password policy into its business application which requires users to reset passwords every 30 days. The help desk is now flooded with password reset requests. Which of the following is the information security manager's BEST course of action to address this situation?

A. Provide end-user training.
B. Escalate to senior management.
C. Continue to enforce the policy.
D. Conduct a business impact analysis (BIA).

Answer: A

Explanation:

Question: 676

When building support for an information security program, which of the following elements is MOST important?

A. Identification of existing vulnerabilities
B. Information risk assessment
C. Business impact analysis (BIA)
D. Threat analysis

Answer: B

Explanation:

Question: 677

A small organization with limited budget hires a new information security manager who finds the same IT staff member is assigned the responsibility of system administrator, security administrator, database administrator (DBA), and application administrator What is the manager's BEST course of action?

A. Automate user provisioning activities.
B. Maintain strict control over user provisioning activities.
C. Formally document IT administrator activities.
D. Implement monitoring of IT administrator activities.

Answer: D

Explanation:

Question: 678

Which of the following is the BEST indicator of an emerging incident?

A. A weakness identified within an organization's information systems
B. Customer complaints about lack of website availability
C. A recent security incident at an industry competitor
D. Attempted patching of systems resulting in errors

Answer: B

Explanation:

Question: 679

Which of the following incident response phases involves actions to help safeguard critical systems while maintaining business operations?

A. Recovery
B. Identification
C. Containment
D. Preparation

Answer: C

Explanation:

Question: 680

Data classification is PRIMARILY the responsibility of:

A. senior management.
B. the data custodian.
C. the data owner.
D. the security manager.

Answer: C

Explanation:

Question: 681

Which of the following is MOST important for an information security manager to consider when identifying information security resource requirements?

A. Current resourcing levels
B. Availability of potential resources
C. Information security strategy
D. Information security incidents

Answer: A

Explanation:

Question: 682

To help users apply appropriate controls related to data privacy regulation, what is MOST important to communicate to the users?

A. Data storage procedures
B. Data classification policy
C. Results of penetration testing
D. Features of data protection products

Answer: B

Explanation:

Question: 683

Which of the following roles is accountable for ensuring the impact of a new regulatory framework on a business system is assessed?

A. Senior management
B. Application owner
C. Information security manager
D. Legal representative

Answer: A

Explanation:

Question: 684

Which of the following is the MOST effective way to address an organizations security concerns during contract negotiations with a third party?

A. Ensure security is involved in the procurement process.
B. Review the third-party contract with the organization's legal department.
C. Conduct an information security audit on the third-party vendor.
D. Communicate security policy with the third-party vendor.

Answer: A

Explanation:

Question: 685

A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ. Which of the following should be evaluated FIRST?

A. Local regulatory requirements
B. Global framework standards
C. Cross-border data mobility
D. Training requirements of the framework

Answer: A

Explanation:

Question: 686

A data loss prevention (DLP) tool has flagged personally identifiable information (PII) during transmission. Which of the following should the information security manager do FIRST?

A. Validate the scope and impact with the business process owner.
B. Initiate the incident response plan.
C. Review and validate the rules within the DLP system.
D. Escalate the issue to senior management.

Answer: A

Explanation:

Question: 687

Which of the following is the PRIMARY reason for executive management to be involved in establishing an enterprise's security management framework?

A. To ensure industry best practices for enterprise security are followed
B. To establish the minimum level of controls needed
C. To determine the desired state of enterprise security
D. To satisfy auditors' recommendations for enterprise security

Answer: C

Explanation:

Question: 688

Which of the following provides the BEST evidence that a newly implemented security awareness program has been effective?

A. Senior management supports funding for ongoing awareness training.
B. Employees from each department have completed the required training.
C. There has been an increase in the number of phishing attempts reported.
D. There have been no reported successful phishing attempts since the training started.

Answer: D

Explanation:

Question: 689

An online trading company discovers that a network attack has penetrated the firewall. What should be the information security manager's FIRST response?

A. Notify the regulatory agency of the incident.
B. Implement mitigating controls.
C. Evaluate the impact to the business.
D. Examine firewall logs to identify the attacker.

Answer: C

Explanation:

Question: 690

After logging in to a web application, additional authentication is checked at various application points. Which of the following is the PRIMARY reason for such an approach?

A. To ensure access rights meet classification requirements
B. To facilitate the analysis of application logs
C. To ensure web application availability
D. To support strong two-factor authentication protocols

Answer: A

Explanation:

Question: 691

Which of the following is a function of the information security steering committee?

A. Deliver external communication during incident response.
B. Align the security framework with security standards.
C. Align security strategy with business objectives.
D. Monitor regulatory requirements.

Answer: C

Explanation:

Question: 692

Which of the following is the MOST important reason for logging firewall activity?

A. Metrics reporting
B. Firewall tuning
C. Intrusion prevention
D. Incident investigation

Answer: C

Explanation:

Question: 693

Several months after the installation of a new firewall with intrusion prevention features to block malicious activity, a breach was discovered that came in through the firewall shortly after installation. This breach could have been detected earlier by implementing firewall:

A. packet filtering.
B. web surfing controls.
C. log monitoring.
D. application awareness.

Answer: C

Explanation:

Question: 694

Which of the following should an information security manager do FIRST upon learning that a competitor has experienced a ransomware attack?

A. Perform a full data backup.
B. Conduct ransomware awareness training for all staff.
C. Update indicators of compromise in the security systems.
D. Review the current risk assessment.

Answer: D

Explanation:

Question: 695

Which of the following metrics would BEST demonstrate the success of a newly implemented information security framework?

A. An increase in the number of identified security incidents
B. A decrease in the number of security audit findings
C. A decrease in the number of security policy exceptions
D. An increase in the number of compliant business processes

Answer: D

Explanation:

Question: 696

An organization has suffered from a large-scale security event impacting a critical system. Following the decision to restore the system at an alternate location, which plan should be invoked?

A. Disaster recovery plan (DRP)
B. Incident response plan
C. Business continuity plan (BCP)
D. Communications plan

Answer: C

Explanation:

Question: 697

Which of the following is the MOST important role of the information security manager when the organization is in the process of adopting emerging technologies?

A. Assessing how peer organizations using the same technologies have been impacted
B. Understanding the impact on existing resources
C. Reviewing vendor contracts and service level agreements (SLAs)
D. Developing training for end users to familiarize them with the new technology

Answer: B

Explanation:

Question: 698

An organization has updated its business goals in the middle of the fiscal year to respond to changes in market conditions. Which of the following is MOST important for the information security manager to update in support of the new goals?

A. Information security threat profile
B. Information security policy
C. Information security objectives
D. Information security strategy

Answer: D

Explanation:

Question: 699

An organization's research department plans to apply machine learning algorithms on a large data set containing customer names and purchase history. The risk of personal data leakage is considered high impact. Which of the following is the BEST risk treatment option in this situation?

A. Accept the risk, as the benefits exceed the potential consequences.
B. Mitigate the risk by applying anonymization on the data set.
C. Transfer the risk by purchasing insurance.
D. Mitigate the risk by encrypting the customer names in the data set.

Answer: B

Explanation:

Question: 700

The PRIMARY purpose of implementing information security governance metrics is to:

A. measure alignment with best practices.
B. assess operational and program metrics.
C. guide security towards the desired state.
D. refine control operations.

Answer: C

Explanation:

Question: 701

Which of the following is the MOST effective way to detect information security incidents?

A. Implementation of regular security awareness programs
B. Periodic analysis of security event log records
C. Threshold settings on key risk indicators (KRIs)
D. Real-time monitoring of network activity

Answer: D

Explanation:

Question: 702

Which of the following is MOST important to include in an information security policy?

A. Best practices
B. Management objectives
C. Baselines
D. Maturity levels

Answer: B

Explanation:

Question: 703

When multiple Internet intrusions on a server are detected, the PRIMARY concern of the information security manager should be to ensure:

A. the integrity of evidence is preserved.
B. forensic investigation software is loaded on the server.
C. the incident is reported to senior management.
D. the server is unplugged from power.

Answer: A

Explanation:

Question: 704

Which or the following is MOST important to consider when determining backup frequency?

A. Recovery point objective (RPO)
B. Recovery time objective (RTO)
C. Allowable interruption window
D. Maximum tolerable outage (MTO)

Answer: A

Explanation:

Question: 705

Which of the following is the BEST way to address data availability concerns when outsourcing information security administration?

A. Develop service level agreements (SLAs).
B. Stipulate insurance requirements.
C. Require nondisclosure agreements (NDAs).
D. Create contingency plans.

Answer: D

Explanation:

Question: 706

What should be the FIRST step when implementing data loss prevention (DLP) technology?

A. Perform due diligence with vendor candidates.
B. Build a business case.
C. Classify the organization's data.
D. Perform a cost-benefit analysis.

Answer: C

Explanation:

Question: 707

In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?

A. Access to the hardware
B. Data encryption
C. Non-standard event logs
D. Compressed customer data

Answer: C

Explanation:

Question: 708

Which of the following would provide the MOST value to senior management when presenting the results of a risk assessment?

A. Mapping the risks to the security classification scheme
B. Illustrating risk on a heat map
C. Mapping the risks to existing controls
D. Providing a technical risk assessment report

Answer: B

Explanation:

Question: 709

Which of the following is the BEST indicator of a successful intrusion into an organization's systems?

A. Decrease in internal network traffic
B. Increase in the number of failed login attempts
C. Increase in the number of irregular application requests
D. Decrease in available storage space

Answer: C

Explanation:

Question: 710

Which of the following BEST enables the restoration of operations after a limited ransomware incident occurs?

A. Reliable image backups
B. Impact assessment
C. Documented eradication procedures
D. Root cause analysis

Answer: A

Explanation:

Question: 711

Which of the following is MOST important to determine following the discovery and eradication of a malware attack?

A. The malware entry path
B. The creator of the malware
C. The type of malware involved
D. The method of detecting the malware

Answer: A

Explanation:

Question: 712

What should a global information security manager do FIRST when informed that a new regulation

with significant impact will go into effect soon?

A. Perform a privacy impact assessment (PIA).
B. Perform a vulnerability assessment.
C. Perform a gap analysis.
D. Perform a business impact analysis (BIA).

Answer: C

Explanation:

Question: 713

An organization has been penalized by regulatory authorities for failing to notify them of a major security breach that may have compromised customer dat

a. Which of the following is MOST likely in need of review and updating to prevent similar penalties in the future?

A. Information security policies and procedures
B. Business continuity plan (BCP)
C. Incident communication plan
D. Incident response training program

Answer: C

Explanation:

Question: 714

The PRIMARY purpose for deploying information security metrics is to:

A. compare program effectiveness to benchmarks.
B. support ongoing security budget requirements.
C. ensure that technical operations meet specifications.
D. provide information needed to make decisions.

Answer: D

Explanation:

Question: 715

The BEST way to report to the board on the effectiveness of the information security program is to present:

A. a dashboard illustrating key performance metrics.
B. a summary of the most recent audit findings.
C. peer-group industry benchmarks.
D. a report of cost savings from process improvements.

Answer: A

Explanation:

Question: 716

Which of the following should be done FIRST when establishing an information security governance

framework?

A. Evaluate information security tools and skills relevant for the environment.
B. Gain an understanding of the business and cultural attributes.
C. Contract a third party to conduct an independent review of the program.
D. Conduct a cost-benefit analysis of the framework.

Answer: B

Explanation:

Question: 717

Which of the following is the BEST way to build a risk-aware culture?

A. Periodically change risk awareness messages.
B. Ensure that threats are documented and communicated in a timely manner.
C. Establish a channel for staff to report risks.
D. Periodically test compliance with security controls.

Answer: C

Explanation:

Question: 718

Which of the following is the MOST important input to the development of an effective information security strategy?

A. Risk and business impact assessments
B. Business processes and requirements
C. Current and desired state of security
D. Well-defined security policies and procedures

Answer: B

Explanation:

Question: 719

Which of the following is the PRIMARY preventive method to mitigate risks associated with privileged accounts?

A. Eliminate privileged accounts.
B. Perform periodic certification of access to privileged accounts.
C. Frequently monitor activities on privileged accounts.
D. Provide privileged account access only to users who need it.

Answer: D

Explanation:

Question: 720

Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?

A. IT strategy
B. Recovery strategy
C. Risk mitigation strategy
D. Security strategy

Answer: B

Explanation:

Question: 721

Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

A. Training project managers on risk assessment
B. Having the information security manager participate on the project steering committees
C. Applying global security standards to the IT projects
D. Integrating the risk assessment into the internal audit program

Answer: B

Explanation:

Question: 722

Which of the following should be implemented to BEST reduce the likelihood of a security breach?

A. A data forensics program
B. A configuration management program
C. A layered security program
D. An incident response program

Answer: C

Explanation:

Question: 723

Which type of plan is PRIMARILY intended to reduce the potential impact of security events that may occur?

A. Security awareness plan
B. Business continuity plan (BCP)
C. Disaster recovery plan (DRP)
D. Incident response plan

Answer: D

Explanation:

Question: 724

Which of the following should be the PRIMARY goal of information security?

A. Information management
B. Regulatory compliance
C. Data governance
D. Business alignment

Answer: D

Explanation:

Question: 725

An experienced information security manager joins a new organization and begins by conducting an audit of all key IT processes. Which of the following findings about the vulnerability management program should be of GREATEST concern?

A. Identified vulnerabilities are not published and communicated in awareness programs.
B. Identified vulnerabilities are not logged and resolved in a timely manner.
C. The number of vulnerabilities identified exceeds industry benchmarks. D. Vulnerabilities are identified by internal staff rather than by external consultants.

Answer: B

Explanation:

Question: 726

A proposal designed to gain buy-in from senior management for a new security project will be MOST effective if it includes:

A. analysis of current threat landscape.
B. historical data of reported incidents.
C. projected return on investment (ROI).
D. industry benchmarking gap analysis.

Answer: C

Explanation:

Question: 727

Which of the following is a PRIMARY function of an incident response team?

A. To provide effective incident mitigation
B. To provide a risk assessment for zero-day vulnerabilities
C. To provide a single point of contact for critical incidents
D. To provide a business impact analysis (BIA)

Answer: A

Explanation:

Question: 728

The PRIMARY goal of a post-incident review should be to:

A. establish the cost of the incident to the business.
B. determine why the incident occurred.
C. identify policy changes to prevent a recurrence.
D. determine how to improve the incident handling process.

Answer: D

Explanation:

Question: 729

Which of the following is the MOST critical consideration when shifting IT operations to an Infrastructure as a Service (laaS) model hosted in a foreign country?

A. Labeling of data may help to ensure data is assigned to the correct cloud type.
B. Laws and regulations of the origin country may not be applicable.
C. There may be liabilities and penalties in the event of a security breach.
D. Data may be stored in unknown locations and may not be easily retrievable.

Answer: B

Explanation:

Question: 730

When remote access is granted to a company's internal network, the MOST important consideration should be that access is provided:

A. on a need-to-know basis subject to controls.
B. subject to legal and regulatory requirements.
C. by the use of a remote access server.
D. if a robust IT infrastructure exists.

Answer: A

Explanation:

Question: 731

Which of the following is MOST important to the effectiveness of an information security steering committee?

A. The committee has strong regulatory knowledge.
B. The committee is comprised of representatives from senior management.
C. The committee has cross-organizational representation.
D. The committee uses a risk management framework.

Answer: C

Explanation:

Question: 732

The PRIMARY purpose of conducting a business impact analysis (BIA) is to determine the:

A. scope of the business continuity program.
B. resources needed for business recovery.
C. recovery time objective (RTO).

D. scope of the incident response plan.

Answer: B

Explanation:

Question: 733

After updating password standards, an information security manager is alerted by various application administrators that the applications they support are incapable of enforcing these standards. The information security manager's FIRST course of action should be to:

A. determine the potential impact.
B. reevaluate the standards.
C. implement compensating controls.
D. evaluate the cost of replacing the applications.

Answer: A

Explanation:

Question: 734

Which of the following is the BEST defense against a brute force attack?

A. Time-of-day restrictions
B. Mandatory access control
C. Discretionary access control
D. Multi-factor authentication (MFA)

Answer: D

Explanation:

Question: 735

Which of the following should be the NEXT step after a security incident has been reported?

A. Recovery
B. Investigation
C. Escalation
D. Containment

Answer: D

Explanation:

Question: 736

Which of the following is the BEST source of information to support an organization's information security vision and strategy?

A. Metrics dashboard
B. Governance policies
C. Capability maturity model
D. Enterprise information security architecture

Answer: D

Explanation:

Question: 737

Which of the following is MOST important to ensuring that incident management plans are executed effectively?

A. Management support and approval has been obtained.
B. The incident response team has the appropriate training.
C. An incident response maturity assessment has been conducted.
D. A reputable managed security services provider has been engaged.

Answer: A

Explanation:

Question: 738

Which of the following is the PRIMARY reason to conduct a post-incident review?

A. To aid in future risk assessments
B. To improve the response process
C. To determine whether digital evidence is admissible
D. To notify regulatory authorities

Answer: B

Explanation:

Question: 739

How does an organization PRIMARILY benefit from the creation of an information security steering committee?

A. An increase in information security risk awareness
B. An increased alignment with industry security trends that impact the business
C. An increased focus on information security resource management
D. An increased alignment of information security with the business

Answer: D

Explanation:

Question: 740

Unintentional behavior by an employee caused a major data loss incident. Which of the following is the BEST way for the information security manager to prevent recurrence within the organization?

A. Implement compensating controls.
B. Communicate consequences for future instances.
C. Enhance the data loss prevention (DLP) solution.
D. Improve the security awareness training program.

Answer: D

Explanation:

Question: 741

Business objectives and organizational risk appetite are MOST useful inputs to the development of information security:

A. strategy.
B. risk assessments.
C. key performance indicators (KPIs).
D. standards.

Answer: A

Explanation:

Question: 742

An information security team plans to strengthen authentication requirements for a customer-facing site, but there are concerns it will negatively impact the user experience. Which of the following is the information security manager's BEST course of action?

A. Assess business impact against security risk.
B. Provide security awareness training to customers.
C. Refer to industry best practices.
D. Quantify the security risk to the business.

Answer: A

Explanation:

Question: 743

When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?

A. Business impact analysis (BIA) results
B. Vulnerability assessment results
C. The business continuity plan (BCP)
D. Recommendations from senior management

Answer: A

Explanation:

Question: 744

Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:

A. hand over the controls to the relevant business owners.
B. ensure the controls are regularly tested for ongoing effectiveness.
C. perform testing to compare control performance against industry levels.
D. prepare to adapt the controls for future system upgrades.

Answer: B

Explanation:

Question: 745

Which of the following should be updated FIRST to account for new regulatory requirements that impact current information security controls?

A. Control matrix
B. Business impact analysis (BIA)
C. Risk register
D. Information security policy

Answer: D

Explanation:

Question: 746

Which of the following is MOST helpful in the development of a cost-effective information security strategy that is aligned with business requirements?

A. Enforcing data retention
B. Developing policy standards
C. Benchmarking against industry peers
D. Categorizing information assets

Answer: C

Explanation:

Question: 747

An information security team must obtain approval from the information security steering committee to implement a key control. Which of the following is the MOST important input to assist the committee in making this decision?

A. IT strategy
B. Security architecture
C. Business case
D. Risk assessment

Answer: C

Explanation:

Question: 748

Which of the following is the GREATEST benefit of performing a tabletop exercise of the business continuity plan (BCP)?

A. It identifies appropriate follow-up work to address shortcomings in the plan.
B. It allows for greater participation and planning from the business side.
C. It helps in assessing the availability of compatible backup hardware.
D. It provides a low-cost method of assessing the BCP's completeness.

Answer: A

Explanation:

Question: 749

Which of the following is MOST helpful in determining whether a phishing email is malicious?

A. Security awareness training
B. Reverse engineering
C. Threat intelligence
D. Sandboxing

Answer: D

Explanation:

Question: 750

Which of the following is the BEST way to reduce the risk associated with a bring your own device (BYOD) program?

A. Implement a mobile device policy and standard.
B. Provide employee training on secure mobile device practices.
C. Implement a mobile device management (MDM) solution.
D. Require employees to install an effective anti-malware app.

Answer: B

Explanation:

Question: 751

Which of the following is the MOST important reason to document information security incidents that are reported across the organization?

A. Evaluate the security posture of the organization.
B. Identify unmitigated risk.
C. Prevent incident recurrence.
D. Support business investments in security.

Answer: C

Explanation:

Question: 752

A financial institution is planning to develop a new mobile application. Which of the following is the BEST time to begin assessments of the application's security compliance?

A. During user acceptance testing (UAT)
B. During the design phase
C. During static code analysis
D. During regulatory review

Answer: B

Explanation:

Question: 753

Which of the following BEST enables an incident response team to determine appropriate actions during an initial investigation?

A. Feedback from affected departments
B. Historical data from past incidents
C. Technical capabilities of the team
D. Procedures for incident triage

Answer: D

Explanation:

Question: 754

An information security manager has learned of an increasing trend in attacks that use phishing emails impersonating an organization's CEO in an attempt to commit wire transfer fraud. Which of the following is the BEST way to reduce the risk associated with this type of attack?

A. Temporarily suspend wire transfers for the organization.
B. Provide awareness training to the CEO for this type of phishing attack.
C. Provide awareness training to staff responsible for wire transfers.
D. Disable emails for staff responsible for wire transfers.

Answer: C

Explanation:

Question: 755

Which of the following is the BEST indication of an effective disaster recovery planning process?

A. Hot sites are required for any declared disaster.
B. Chain of custody is maintained throughout the disaster recovery process.
C. Post-incident reviews are conducted after each event.
D. Recovery time objectives (RTOs) are shorter than recovery point objectives (RPOs).

Answer: C

Explanation:

Question: 756

Which of the following is MOST important for the information security manager to include when presenting changes in the security risk profile to senior management?

A. Industry benchmarks
B. Security training test results
C. Performance measures for existing controls
D. Number of false positives

Answer: C

Explanation:

Question: 757

Following an unsuccessful denial of service (DoS) attack, identified weaknesses should be:

A. quickly resolved and eliminated regardless of cost.
B. tracked and reported on until their final resolution.
C. documented in security awareness programs.
D. noted and re-examined later if similar weaknesses are found.

Answer: D

Explanation:

Question: 758

The PRIMARY reason to properly classify information assets is to determine:

A. appropriate encryption strength using a risk-based approach.
B. the business impact if assets are compromised.
C. the appropriate protection based on sensitivity.
D. user access levels based on the need to know.

Answer: C

Explanation:

Question: 759

Which of the following should be done FIRST when developing a business continuity plan (BCP)?

A. Review current recovery policies.
B. Define the organizational strategy.
C. Prioritize the critical processes.
D. Review existing cyber insurance coverage.

Answer: B

Explanation:

Question: 760

Which of the following would be the GREATEST obstacle to implementing incident notification and escalation processes in an organization with high turnover?

A. Lack of knowledgeable personnel

B. Lack of communication processes
C. Lack of process documentation
D. Lack of alignment with organizational goals

Answer: A

Explanation:

Question: 761

Which of the following processes is MOST important for the success of a business continuity plan (BCP)?

A. Involving all stakeholders in testing and training
B. Scheduling periodic internal and external audits
C. Including the board and senior management in plan reviews
D. Maintaining copies of the plan at the primary and recovery sites

Answer: A

Explanation:

Question: 762

When analyzing the emerging risk and threat landscape, an information security manager should FIRST:

A. determine the impact if threats materialize.
B. determine the sources of emerging threats.
C. review historical threats within the industry.
D. map threats to business assets.

Answer: B

Explanation:

Question: 763

What should be the NEXT course of action when an information security manager has identified a department that is repeatedly not following the security policy?

A. Perform a vulnerability assessment on the systems within the department.
B. Introduce additional controls to force compliance with policy.
C. Require department users to repeat security awareness training.
D. Report the policy violation to senior management.

Answer: D

Explanation:

Question: 764

Which of the following is MOST important for an information security manager to consider when determining whether data should be stored?

A. Data protection regulations
B. Data storage limitations
C. Business requirements
D. Type and nature of data

Answer: C

Explanation:

Question: 765

Which of the following is the MOST important characteristic of an effective information security metric?

A. The metric expresses residual risk relative to risk tolerance.
B. The metric is frequently reported to senior management.
C. The metric directly maps to an industry risk management framework.
D. The metric compares the organization's inherent risk against its risk appetite.

Answer: A

Explanation:

Question: 766

Which of the following should an organization do FIRST upon learning that a subsidiary is located in a country where civil unrest has just begun?

A. Assess changes in the risk profile.
B. Activate the disaster recovery plan (DRP).
C. Invoke the incident response plan.
D. Conduct security awareness training.

Answer: A

Explanation:

Question: 767

Senior management recently approved a mobile access policy that conflicts with industry best practices. Which of the following is the information security manager's BEST course of action when developing security standards for mobile access to the organization's network?

A. Align the standards with the organizational policy.
B. Align the standards with industry best practices.
C. Resolve the discrepancy before developing the standards.
D. Perform a cost-benefit analysis of aligning the standards to policy.

Answer: C

Explanation:

The Information Security Manager's primary responsibility is to ensure that the organization's information assets are adequately protected. In this scenario, there is a conflict between the approved mobile access policy and industry best practices. Developing security standards based on a flawed policy could lead to significant security vulnerabilities.

Why the other options are not the best course of action:

A . Align the standards with the organizational policy: This would perpetuate the misalignment with best practices, potentially leaving the organization exposed to risks.

B . Align the standards with industry best practices: While this is ideal from a security perspective, it directly contradicts the approved policy, which could create operational and compliance issues.

D . Perform a cost-benefit analysis of aligning the standards to policy: A cost-benefit analysis might be useful at some point, but it does not address the fundamental issue of a policy that is not in line with best practices.

Key CISM Principles Reflected:

Alignment with Organizational Objectives: Security standards and policies should support and enable the organization's business objectives.

Risk Management: Identifying, assessing, and mitigating risks are essential elements of information security management.

Governance: Effective governance ensures that information security activities are aligned with the organization's strategies and objectives.

In summary: The Information Security Manager should proactively engage senior management to highlight the discrepancy between the approved policy and industry best practices. The goal is to revise the policy to ensure it adequately addresses security risks while supporting the organization's objectives. Once the policy is aligned with best practices, the security standards can be developed accordingly.

Question: 768

Which of the following metrics would provide an accurate measure of an information security program's performance?

A. A collection of qualitative indicators that accurately measure security exceptions
B. A combination of qualitative and quantitative trends that enable decision making
C. A collection of quantitative indicators that are compared against industry benchmarks

D. A single numeric score derived from various measures assigned to the security program

Answer: A

Explanation:

Question: 769

Which of the following is the PRIMARY reason that an information security manager should restrict the use of generic administrator accounts in a multi-user environment?

A. To ensure separation of duties is maintained
B. To ensure system audit trails are not bypassed
C. To prevent accountability issues
D. To prevent unauthorized user access

Answer: C

Explanation:

Question: 770

For event logs to be acceptable for incident investigation, which of the following is the MOST important consideration to establish chain of evidence?

A. Centralized logging
B. Time clock synchronization
C. Available forensic tools
D. Administrator log access

Answer: B

Explanation:

Question: 771

Which of the following provides the BEST input to determine the level of protection needed for an IT system?

A. Vulnerability assessment
B. Asset classification
C. Threat analysis
D. Internal audit findings

Answer: B

Explanation:

Question: 772

Identifying which of the following BEST enables a cyberattack to be contained?

A. The vulnerability exploited by the attack
B. The segment targeted by the attack
C. The IP address of the computer that launched the attack
D. The threat actor that initiated the attack

Answer: B

Explanation:

Question: 773

Which of the following is the BEST way to compete for funding for an information security program in an organization with limited resources?

A. Demonstrate the effectiveness of business continuity plans (BCPs).
B. Report key performance indicator (KPI) trends.
C. Demonstrate that the program enables business activities.
D. Provide evidence of increased security events at peer organizations.

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step
The goal of securing funding for an information security program often requires aligning the program with business goals and demonstrating its value to the organization. Here's an analysis of each option:
A . Demonstrate the effectiveness of business continuity plans (BCPs): While important, this focuses on continuity rather than the overall value of the information security program to business objectives. This is not the strongest method to justify funding.
B . Report key performance indicator (KPI) trends: KPI trends are useful for tracking performance but may not directly demonstrate how the program supports business activities or adds value.
C . Demonstrate that the program enables business activities: This is the BEST option because it ties the information security program directly to business operations. When security is seen as an enabler (e.g., reducing risks in critical areas like customer data protection), stakeholders are more likely to allocate resources.
D . Provide evidence of increased security events at peer organizations: This may indicate a general threat landscape but does not provide concrete evidence of the program's value or relevance to the organization's specific goals.

Reference: CISM Job Practice Area 1 (Information Security Governance) emphasizes aligning information security strategies with organizational objectives to gain stakeholder support.

Question: 774

Which type of backup BEST enables an organization to recover data after a ransomware attack?

A. Online backup
B. Incremental backup
C. Differential backup
D. Ofline backup

Answer: D

Explanation:

Comprehensive and Detailed Step-by-Step

Recovering from ransomware requires backups that are unaffected by the ransomware attack. Here's why ofline backups are most effective:

A . Online backup: These are connected to the network and may also be compromised during an attack.

B . Incremental backup: While efficient, incremental backups rely on previous backups and are typically stored online, making them vulnerable to ransomware.

C . Differential backup: Similar to incremental backups, these are not immune if stored online or on compromised systems.

D . Ofline backup: This is the BEST choice as ofline backups are stored in a location that is not connected to the network, preventing ransomware from encrypting them.

Reference: CISM Job Practice Area 4 (Information Security Incident Management) includes guidance on establishing robust backup strategies for recovery.

Question: 775

An organization is selecting security metrics to measure security performance, and a firewall specialist suggests tracking the number of external attacks blocked by the firewalls. Which of the following is the GREATEST concern with using this metric?

A. The number of blocked external attacks is not representative of the true threat profile.
B. The number of blocked external attacks will vary by month, causing inconsistent graphs.
C. The number of blocked external attacks is an indicator of the organization's popularity.
D. The number of blocked external attacks over time does not explain the attackers' motivations.

Answer: A

Explanation:

Comprehensive and Detailed Step-by-Step

Metrics should provide meaningful insights into the organization's risk exposure and security performance.

Evaluating this option:

A . The number of blocked external attacks is not representative of the true threat profile: This is the BEST answer because counting attacks blocked does not reveal the effectiveness of security controls or the real risk environment.

B . The number of blocked external attacks will vary by month, causing inconsistent graphs: While variability is a concern, it does not make the metric invalid.

C . The number of blocked external attacks is an indicator of the organization's popularity: This is true but irrelevant to assessing the effectiveness of security measures.

D . The number of blocked external attacks over time does not explain the attackers' motivations: Understanding motivations is useful but not directly tied to evaluating the firewall metric's effectiveness.

Reference: CISM Job Practice Area 2 (Risk Management) emphasizes the need for meaningful and risk-based metrics.

Question: 776

Which of the following provides the MOST effective response against ransomware attacks?

A. Automatic quarantine of systems
B. Thorough communication plans
C. Effective backup plans and processes
D. Strong password requirements

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step

Recovering from ransomware attacks often depends on having a robust data recovery strategy:

A . Automatic quarantine of systems: This can limit the spread of ransomware but does not address recovery.

B . Thorough communication plans: Communication is important during incidents but does not directly mitigate ransomware.

C . Effective backup plans and processes: This is the BEST option because having backups ensures that encrypted data can be restored, minimizing downtime and data loss.

D . Strong password requirements: This helps prevent unauthorized access but is not sufficient to combat ransomware once it has entered the system.

Reference: CISM Job Practice Area 4 (Information Security Incident Management) stresses the importance of backup and recovery strategies to mitigate ransomware risks.

Question: 777

Which of the following is the BEST tool to use for identifying and correlating intrusion attempt alerts?

A. Threat analytics software
B. Host intrusion detection system
C. SIEM
D. Network intrusion detection system

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step

Security Information and Event Management (SIEM) systems are designed to collect, analyze, and correlate data from multiple sources, making them the BEST choice for identifying and correlating intrusion attempt alerts.

A . Threat analytics software: While this can provide insights, it is not specialized for real-time correlation and alerting across various platforms.

B . Host intrusion detection system (HIDS): HIDS monitors individual hosts and detects intrusions, but it does not correlate alerts from multiple sources.

C . SIEM: This is the BEST answer because SIEM integrates logs from diverse systems, applies correlation rules, and provides actionable insights into intrusion attempts.

D . Network intrusion detection system (NIDS): While NIDS detects network-level anomalies, it does not correlate alerts from other systems.

Reference: CISM Job Practice Area 3 (Information Security Program Development and Management) discusses tools and techniques for monitoring and detecting security events.

Question: 778

An incident response policy should include:

A. A description of testing methodology.
B. Notification requirements.
C. An infrastructure diagram.
D. Recovery time objectives (RTOs).

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step

Incident response policies must provide clear and actionable steps to ensure effective handling of incidents. Notification requirements are critical to ensure timely communication with stakeholders during an incident.

A . A description of testing methodology: While testing is important, it is typically addressed in incident response plans, not the policy itself.

B . Notification requirements: This is the BEST answer as it ensures that key stakeholders are informed promptly, allowing for coordination and mitigation efforts.

C . An infrastructure diagram: This is useful for understanding system architecture but is not a core policy requirement.

D . Recovery time objectives (RTOs): RTOs are part of business continuity and disaster recovery plans, not incident response policies.

Reference: CISM Job Practice Area 4 (Information Security Incident Management) emphasizes the importance of clear communication and notification procedures in incident response.

Question: 779

Which of the following would be MOST important to include in a proposal justifying investments for an organization's information security program?

A. Vulnerability scan results
B. Competitor benchmark analysis
C. Previous security budget
D. Business requirements

Answer: D

Explanation:

Comprehensive and Detailed Step-by-Step

Justifying investments in information security requires aligning proposals with business objectives to gain management approval.

A . Vulnerability scan results: These provide technical insights but are insufficient for high-level justification.

B . Competitor benchmark analysis: While useful, this is less relevant than demonstrating direct alignment with organizational needs.

C . Previous security budget: Historical data may provide context but does not justify future needs.

D . Business requirements: This is the BEST answer because aligning security investments with business objectives demonstrates the value and necessity of the program to stakeholders.

Reference: CISM Job Practice Area 1 (Information Security Governance) focuses on aligning security initiatives with business goals to secure buy-in.

Question: 780

Which of the following is the BEST indication of an effective information security program?

A. Risk is treated to an acceptable level.
B. The number of security incidents reported by staff has increased.
C. Key risk indicators (KRIs) are established.
D. Policies are reviewed and approved by senior management.

Answer: A

Explanation:

Comprehensive and Detailed Step-by-Step

An effective information security program aims to manage risks to acceptable levels while supporting business objectives.

A . Risk is treated to an acceptable level: This is the BEST answer as it directly reflects the program's success in mitigating risks within the organization's tolerance levels.

B . The number of security incidents reported by staff has increased: An increase in reported incidents might indicate improved awareness but does not necessarily reflect overall effectiveness. C . Key risk indicators (KRIs)

are established: KRIs are important for monitoring risks but do not indicate whether risks are being effectively managed.

D . Policies are reviewed and approved by senior management: While essential, this action alone does not demonstrate the program's effectiveness.

Reference: CISM Job Practice Area 2 (Risk Management) highlights the importance of risk treatment and its alignment with organizational risk tolerance.

Question: 781

Which of the following is CRITICAL to ensure the appropriate stakeholder makes decisions during a cybersecurity incident?

A. Stakeholder plan
B. Escalation plan
C. Up-to-date risk register
D. Asset classification

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step

During a cybersecurity incident, it is vital to ensure that the right people are involved and that decision-making occurs promptly.

A . Stakeholder plan: While identifying stakeholders is important, it does not outline decision-making during an incident.

B . Escalation plan: This is the BEST answer because it specifies how incidents are escalated to the appropriate level of authority, ensuring timely and effective decisions.

C . Up-to-date risk register: Although useful for understanding risks, it does not facilitate decisionmaking in real-time incidents.

D . Asset classification: This helps identify critical assets but does not address decision-making protocols during an incident.

Reference: CISM Job Practice Area 4 (Information Security Incident Management) highlights the importance of escalation procedures to manage incidents efficiently.

Question: 782

When taking a risk-based approach to vulnerability management, which of the following is MOST important to consider when prioritizing a vulnerability?

A. The information available about the vulnerability
B. The sensitivity of the asset and the data it contains
C. IT resource availability and constraints
D. Whether patches have been developed and tested

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step

Risk-based vulnerability management prioritizes vulnerabilities based on the potential impact on critical assets.

A . The information available about the vulnerability: While important for assessing risk, it does not directly determine the priority.

B . The sensitivity of the asset and the data it contains: This is the BEST answer because prioritizing vulnerabilities based on the criticality of the affected assets ensures that high-impact threats are addressed first.

C . IT resource availability and constraints: These are logistical considerations but should not outweigh risk impact.

D . Whether patches have been developed and tested: Patches are important for remediation but do not determine prioritization.

Reference: CISM Job Practice Area 2 (Risk Management) emphasizes considering asset criticality when prioritizing vulnerabilities.

Question: 783

Which of the following BEST enables an organization to determine the costs of downtime for a critical application?

A. Fault tree analysis
B. Cost-benefit analysis
C. Return on investment (ROI) analysis
D. Business impact analysis (BIA)

Answer: D

Explanation:

Comprehensive and Detailed Step-by-Step

Determining downtime costs requires understanding the financial and operational impact on the business.

A . Fault tree analysis: Primarily used for identifying the root causes of failures, not for assessing downtime costs.

B . Cost-benefit analysis: Compares the costs and benefits of implementing controls but does not specifically address downtime.

C . Return on investment (ROI) analysis: Evaluates the financial return of an investment rather than the cost of an outage.

D . Business impact analysis (BIA): This is the BEST answer because a BIA identifies the effects of a disruption on critical business functions and quantifies the financial impact, including downtime costs.

Reference: CISM Job Practice Area 3 (Information Security Program Development and Management) discusses BIA as a key component in understanding the financial implications of downtime.

Question: 784

Which of the following is the PRIMARY reason to review the firewall logs when an external networkbased attack is reported by the intrusion detection system (IDS)?

A. To validate the incident
B. To review network configurations
C. To validate the payload signature
D. To devise the incident response strategy

Answer: A

Explanation:

Question: 785

An organization is MOST likely to accept the risk of noncompliance with a new regulatory requirement when:

A. employees are resistant to the controls required by the new regulation.
B. the regulatory requirement conflicts with business requirements.
C. the risk of noncompliance exceeds the organization's risk appetite.
D. the cost of complying with the regulation exceeds the potential penalties.

Answer: D

Explanation:

An organization is most likely to accept the risk of noncompliance with a new regulatory requirement when the cost of complying with the regulation exceeds the potential penalties. In such cases, from a cost-benefit perspective, the organization might find it more economical to absorb potential fines or penalties rather than implementing costly controls or processes to comply with the regulation.
"Risk acceptance occurs when the cost of mitigating or transferring the risk exceeds the benefit of the mitigation. This also applies to regulatory noncompliance if the penalties are less than the costs of compliance."
— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options*
ISACA's practice questions highlight that risk acceptance is a legitimate treatment when costs outweigh potential penalties or impact.

Question: 786

What is the MOST important consideration for an organization operating in a highly regulated market when new regulatory requirements with high impact to the business need to be implemented?

A. Engaging an external audit

B. Establishing compensating controls
C. Enforcing strong monitoring controls
D. Conducting a gap analysis

Answer: D

Explanation:

Question: 787

Who is accountable for ensuring proper controls are in place to address the confidentiality and availability of an information system?

A. Senior management
B. Information owner
C. Business manager
D. Information security manager

Answer: A

Explanation:

Question: 788

The MOST effective tools for responding to new and advanced attacks are those that detect attacks based on:

A. signature analysis.
B. behavior analysis.
C. penetration testing.
D. data packet analysis.

Answer: B

Explanation:

Question: 789

What will BEST facilitate the success of new security initiatives?

A. Establish an IT security steering committee.
B. Include business in security decision making.
C. Update security policies on a regular basis

D. Monitor post-implementation security metrics.

Answer: B

Explanation:

Question: 790

Which of the following is MOST important when designing an information security governance framework?

A. Aligning with the information security strategy
B. Assessing the availability of information security resources
C. Aligning with industry best practice frameworks
D. Assessing the current state of information security

Answer: A

Explanation:

Question: 791

Which of the following is MOST important for an information security manager to consider when reviewing a security investment plan?

A. The plan has summarized IT costs for implementation.
B. The plan resolves all potential threats to business processes.
C. The plan focuses on meeting industry best practices and industry standards.
D. The plan is based on a review of threats and vulnerabilities.

Answer: D

Explanation:

Question: 792

An organization engages a third-party vendor to monitor and support a financial application under scrutiny by regulators. Which of the following controls would MOST effectively manage risk to the organization?

A. Implementing separation of duties between systems and data
B. Including penalty clauses for noncompliance in the vendor contract
C. Disabling vendor access and only re-enabling when access is needed
D. Monitoring key risk indicators (KRIs)

Answer: D

Explanation:

Question: 793

What should an information security manager do FIRST when an organization is planning to use a third-party cloud computing service for a critical business process?

A. Identify the data to be hosted.
B. Perform a gap analysis.
C. Perform a risk assessment.
D. Analyze the business requirements.

Answer: B

Explanation:

Question: 794

Which of the following should be done FIRST after a ransomware incident has been successfully contained?

A. Notify relevant stakeholders.
B. Conduct forensic analysis.
C. Perform lessons learned.
D. Restore impacted systems.

Answer: A

Explanation:

Question: 795

A new type of ransomware has infected an organization's network. Which of the following would have BEST enabled the organization to detect this situation?

A. Regular review of the threat landscape
B. Periodic information security training for end users
C. Use of integrated patch deployment tools
D. Monitoring of anomalies in system behavior

Answer: D

Explanation:

Question: 796

If the investigation of an incident is not completed within the time allocated in the incident response plan, which of the following actions should be taken by the incident response team?

A. Initiate the escalation process.
B. Continue the investigation.
C. Invoke the business continuity plan (BCP).
D. Engage the crisis management team.

Answer: A

Explanation:

Question: 797

An organization has determined that fixing a security vulnerability in a critical application is too costly to be feasible, but the impact is material to the business. Which of the following is the MOST appropriate risk treatment?

A. Purchase cybersecurity insurance.
B. Accept the risk associated with continued use of the application.
C. Implement compensating controls for the application.
D. Discontinue using the application.

Answer: C

Explanation:

Question: 798

Which of the following should an information security manager do FIRST when noncompliance with security standards is identified?

A. Report the noncompliance to senior management.
B. Validate the noncompliance.
C. Include the noncompliance in the risk register.
D. Implement compensating controls to mitigate the noncompliance.

Answer: B

Explanation:

Question: 799

Which of the following BEST determines the data retention strategy and subsequent policy for an organization?

A. Business impact analysis (BIA)
B. Business requirements
C. Supplier requirements
D. Risk appetite

Answer: B

Explanation:

Question: 800

When selecting metrics to monitor the effectiveness of an information security program, it is MOST important for an information security manager to:

A. consider the organizations business strategy.
B. consider the strategic objectives of the program.
C. leverage industry benchmarks.
D. identify the program's risk and compensating controls.

Answer: B

Explanation:

Question: 801

Which of the following is the BEST method for determining whether new risks exist in legacy systems?

A. Frequent updates to the risk register
B. Regularly scheduled security audits
C. Frequent security architecture reviews
D. Regularly scheduled risk assessments

Answer: D

Explanation:

Question: 802

Of the following, who should be assigned as the owner of a newly identified risk related to an organization's new payroll system?

A. Data privacy officer
B. Information security manager
C. Head of IT department
D. Head of human resources (HR)

Answer: D

Explanation:

Question: 803

Which of the following should be done FIRST to prioritize response to incidents?

A. Containment
B. Escalation
C. Analysis
D. Triage

Answer: A

Explanation:

Question: 804

Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?

A. Forensics certification
B. Disaster recovery drills
C. Tabletop exercises
D. Penetration tests

Answer: C

Explanation:

Question: 805

A startup company deployed several new applications with vulnerabilities into production because security reviews were not conducted. What will BEST help to ensure effective application risk management going

forward?

A. Conduct automated scans on applications before deployment.
B. Supplement existing development teams with security engineers.
C. Integrate information security into existing change management.
D. Create a new governance council for application security.

Answer: C

Explanation:

Integrating information security into existing change management processes ensures that security considerations are included in all application changes and deployments. This addresses the root cause of bypassed security reviews and provides a consistent, repeatable process to manage risk going forward.
"Integrating security into change management ensures that changes to systems and applications undergo appropriate security review and testing prior to implementation, thereby addressing vulnerabilities proactively."
— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Change Management*

Question: 806

Which of the following is an example of a change to the external threat landscape?

A. The information security program has been outsourced.
B. A commonly used encryption algorithm has been compromised.
C. Industry security standards have been modified.
D. The organization has been purchased by another entity.

Answer: D

Explanation:

Question: 807

Information security policies should PRIMARILY reflect alignment with:

A. an information security framework.
B. industry best practices.
C. data security standards.
D. senior management intent.

Answer: D

Explanation:

Question: 808

Which of the following is the BEST way to prevent insider threats?

A. Enforce separation of duties and least privilege access.
B. Conduct organization-wide security awareness training.
C. Implement logging for all access activities.
D. Implement strict security policies and password controls.

Answer: C

Explanation:

Question: 809

Which of the following is established during the preparation phase of an incident response plan?

A. Recovery time objectives (RTOs)
B. Chain of custody procedures
C. Stakeholder communication plan
D. Mean time to respond (MTTR)

Answer: C

Explanation:

Question: 810

An organization has identified IT failures in a call center application. Of the following, who should own this risk?

A. Information security manager
B. Head of the call center
C. Chief executive officer (CEO)
D. Head of the IT department

Answer: B

Explanation:

Question: 811

An information security manager has been made aware of a new data protection regulation that will soon go

into effect. Which of the following is the BEST way to manage the risk of noncompliance?

A. Perform a gap analysis.
B. Consult with senior management on the best course of action.
C. Implement a program of work to comply with the new legislation.
D. Understand the cost of noncompliance.

Answer: A

Explanation:

Question: 812

Which of the following is the MOST important reason to involve external forensics experts in evidence collection when responding to a major security breach?

A. To ensure evidence is handled by qualified resources
B. To validate the incident response process
C. To provide the response team with expert training on evidence handling
D. To prevent evidence from being disclosed to any internal staff members

Answer: A

Explanation:

Question: 813

Which of the following is MOST important for the successful implementation of an incident response plan?

A. Ensuring response staff are appropriately trained
B. Developing metrics for incident response reporting
C. Establishing an escalation process for the help desk D. Developing a RACI chart of response staff functions

Answer: A

Explanation:

Question: 814

Which of the following is MOST important to ensure the alignment of an information security program with the organizational strategy?

A. Benchmarking against industry peers

B. Adoption of an industry recognized framework
C. Approval from senior management
D. Identification of business-specific risk factors

Answer: C

Explanation:

Question: 815

Which of the following will BEST facilitate integrating the information security program into corporate governance?

A. An up-to-date security strategy
B. Documentation of the threat landscape
C. Documentation of residual risk
D. A minimum security baseline

Answer: A

Explanation:

Question: 816

Which of the following is the PRIMARY responsibility of an information security governance committee?

A. Discussing upcoming information security projects
B. Reviewing the information security risk register
C. Approving changes to the information security strategy
D. Reviewing monthly information security metrics

Answer: C

Explanation:

Question: 817

Which of the following is the MOST appropriate risk response when the risk impact has been determined to be immaterial and the likelihood is very low?

A. Mitigate
B. Avoid
C. Transfer

D. Accept

Answer: D

Explanation:

Question: 818

Which of the following activities is MOST appropriate to conduct during the eradication phase of a cyber incident response?

A. Restore affected systems for normal operations.
B. Mitigate exploited vulnerabilities to stop future incidents.
C. Estimate the amount of damage caused by the incident.
D. Isolate affected systems to prevent further damage

Answer: B

Explanation:

Question: 819

Which of the following is an information security manager's BEST recommendation to senior management following a breach at the organization's Software as a Service (SaaS) vendor?

A. Update the vendor risk assessment.
B. Engage legal counsel.
C. Renegotiate the vendor contract.
D. Terminate the relationship with the vendor.

Answer: A

Explanation:

Question: 820

Which of the following BEST enables an organization to continuously assess the information security risk posture?

A. Key risk indicators (KRIs)
B. Periodic review of the risk register
C. Degree of senior management support
D. Compliance with industry regulations

Answer: A

Explanation:

Question: 821

Which of the following is MOST relevant for an information security manager to communicate to the board of directors?

A. The level of inherent risk
B. Vulnerability assessments
C. The level of exposure
D. Threat assessments

Answer: C

Explanation:

Question: 822

Which of the following is the MOST important reason to consider organizational culture when developing an information security program?

A. Everyone in the organization is responsible for information security.
B. It helps expedite approval for the information security budget.
C. It helps the organization meet compliance requirements.
D. Security incidents have an adverse impact on the entire organization.

Answer: A

Explanation:

Question: 823

Of the following, who would provide the MOST relevant input when aligning the information security strategy with organizational goals?

A. Enterprise risk committee
B. Information security steering committee
C. Data privacy officer (DPO)
D. Chief information security officer (CISO)

Answer: D

Explanation:

Question: 824

Which of the following is MOST helpful to identify whether information security policies have been followed?

A. Preventive controls
B. Detective controls
C. Directive controls
D. Corrective controls

Answer: B

Explanation:

Question: 825

Which of the following is the MOST likely reason for a vulnerability scanner to return incomplete results?

A. Unauthenticated vulnerability scans are being performed.
B. Scan results are not ingested into a security information and event management (SIEM) tool.
C. Host names have not been fully enumerated.
D. Zero-day vulnerability signatures have not been ingested.

Answer: A

Explanation:

Question: 826

Which of the following should be the KEY consideration when creating an information security communication plan with industry peers?

A. Balancing the benefits of information sharing with the drawbacks of sharing sensitive information
B. Reducing the costs associated with information sharing by automating the process
C. Ensuring information is detailed enough to be of use to other organizations
D. Notifying the legal department whenever incident-related information is shared

Answer: A

Explanation:

Question: 827

Which of the following is the FIRST step in developing a business continuity plan (BCP)?

A. Determine the business recovery strategy
B. Determine available resources.
C. Identify the applications with the shortest recovery time objectives (RTOs).
D. Identify critical business processes.

Answer: D

Explanation:

Question: 828

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Implement a SIEM solution.
B. Perform a threat analysis.
C. Establish performance metrics for the team.
D. Perform a post-incident review.

Answer: D

Explanation:

Question: 829

Which of the following is the BEST reason to implement an information security architecture?

A. Assess the cost-effectiveness of the integration.
B. Fast-track the deployment of information security components.
C. Serve as a post-deployment information security road map.
D. Facilitate consistent implementation of security requirements.

Answer: D

Explanation:

Question: 830

An employee who is a remote user has copied financial data from the corporate server to a laptop using virtual

private network (VPN) connectivity. Which of the following is the MOST important factor to determine if it should be classified as a data leakage incident?

A. Review of the audit logs
B. Ownership of the data
C. Employee's job role
D. Valid use case

Answer: D

Explanation:

Question: 831

An organization has just updated its backup capability to a new cloud-based solution. Which of the following tests will MOST effectively verify this change is working as intended?

A. Tabletop testing
B. Black box testing
C. Parallel testing
D. Simulation testing

Answer: C

Explanation:

Question: 832

A global organization is planning to expand its operations into a new country with stricter data protection regulations than those in the headquarters' home country. Which of the following is the BEST approach for adopting these new requirements?

A. Adjust organization-wide security polices to align with regulations of the new country.
B. Ensure local operations comply with geographical data protection laws of the headquarters.
C. Work with legal to interpret the local regulatory requirements and implement applicable controls.
D. Procure cybersecurity insurance that covers potential breaches and incidents in the new country.

Answer: C

Explanation:

Question: 833

Which of the following BEST enables an information security manager to demonstrate the effectiveness of the

information security and risk program to senior management?

A. Updated risk assessments
B. Counts of information security incidents
C. Audit reports
D. Monthly metrics

Answer: D

Explanation:

Question: 834

Which of the following is an information security manager's MOST important course of action after receiving information about a new cybersecurity threat?

A. Assess the impact of the new threat on the organization in the event of materialization.
B. Update correlation rules for log monitoring to detect the possible emerging threat.
C. Report the threat to senior management immediately to enable an informed decision.
D. Review the enterprise architecture (EA) for vulnerabilities exploited by the threat.

Answer: A

Explanation:

Question: 835

An organization would like to invest in a new emerging technology. Which of the following is MOST important for the information security manager to consider when evaluating its impact?

A. Secure configuration
B. Vulnerabilities in the technology
C. Systems compatibility
D. Industry peer reviews of the technology

Answer: B

Explanation:

Question: 836

Which of the following is the BEST course of action when using a web application that has known vulnerabilities?

A. Monitor application level logs.

B. Deploy host-based intrusion detection.
C. Deploy an application firewall.
D. Install anti-spyware software.

Answer: C

Explanation:

Question: 837

An incident response plan is being developed for servers hosting sensitive information. In the event of a breach, who should make the decision to shut down the system?

A. Operations manager
B. Service owner
C. Information security manager
D. Incident response team

Answer: C

Explanation:

Question: 838

Which of the following is MOST important to have in place when conducting a security control assessment of a system?

A. Control specifications
B. Assurance test plan
C. Scanning tools
D. Security documentation

Answer: A

Explanation:

Question: 839

A business continuity plan (BCP) should contain:

A. information about eradication activities.
B. hardware and software inventories.
C. data restoration procedures.
D. criteria for activation.

Answer: D

Explanation:

Question: 840

Which of the following BEST supports investments in an information security program?

A. Business cases
B. Business impact analysis (BIA)
C. Gap analysis results
D. Risk assessment results

Answer: D

Explanation:

Question: 841

An information security manager has been notified that two senior executives have the ability to elevate their own privileges in the corporate accounting system, in violation of policy. What is the FIRST step to address this issue?

A. Immediately suspend the executives' access privileges.
B. Notify the CISO of the security policy violation.
C. Perform a full review of all system transactions over the past 90 days.
D. Perform a system access review.

Answer: D

Explanation:

Question: 842

Detailed business continuity plans (BCPs) should be PRIMARILY based on:

A. strategies validated by senior management.
B. capabilities of available local vendors.
C. strategies that cover all applications.
D. cost and resources needed to execute.

Answer: A

Explanation:

Question: 843

A business impact analysis (BIA) BEST enables an organization to establish:

A. annualized loss expectancy (ALE).
B. recovery methods.
C. total cost of ownership (TCO).
D. restoration priorities.

Answer: D

Explanation:

Question: 844

Which of the following is the PRIMARY reason for an information security manager to periodically review existing controls?

A. To prioritize security initiatives
B. To avoid redundant controls
C. To align with emerging risk
D. To address end-user control complaints

Answer: C

Explanation:

Question: 845

Which type of control is an incident response team?

A. Preventive
B. Detective
C. Corrective
D. Directive

Answer: C

Explanation:

Question: 846

An information security manager has confirmed the organization's cloud provider has unintentionally published some of the organization's business dat

a. Which of the following should be done NEXT?

A. Identify users associated with the exposed data.
B. Initiate the organization's data loss prevention (DLP) processes.
C. Review the cloud provider's service level agreement (SLA).
D. Invoke the incident response plan.

Answer: D

Explanation:

Question: 847

Which of the following is the PRIMARY reason to use a phased incident recovery approach?

A. To gain management buy-in
B. To give the response team time to analyze incidents
C. To ensure critical systems are recovered first
D. To prioritize remediation steps

Answer: C

Explanation:

Question: 848

Which of the following will BEST enable an organization to meet incident response requirements when outsourcing its incident response function?

A. Including response times in service level agreements (SLAs)
B. Including a right-to-audit clause in service level agreements (SLAs)
C. Contracting with a well-known incident response provider
D. Requiring comprehensive response applications and tools

Answer: B

Explanation:

Question: 849

An organization successfully responded to an information security incident. However, the information security manager learned that some of the steps specified in the incident management procedures were not taken by the response team. What should be the information security manager's FIRST step?

A. Provide additional training to the incident response team.
B. Review the incident management procedures.
C. Interview the incident response team.
D. Remove the steps from the incident management procedures.

Answer: C

Explanation:

Question: 850

During a post-incident review, it was determined that a known vulnerability was exploited in order to gain access to a system. The vulnerability was patched as part of the remediation on the offending system. Which of the following should be done NEXT?

A. Install patches on all existing systems.
B. Review the vulnerability management process.
C. Report the root cause of the vulnerability to senior management.
D. Scan to determine whether the vulnerability is present on other systems.

Answer: D

Explanation:

Question: 851

A data discovery project uncovers an unclassified process document. Of the following, who is BEST suited to determine the classification?

A. Information security manager
B. Security policy author
C. Creator of the document
D. Data custodian

Answer: C

Explanation:

Question: 852

Which of the following is MOST important for an information security manager to consider when developing a business continuity plan (BCP) for ransomware attacks?

A. Backups are maintained ofline and regularly tested.
B. Impacted networks can be detached at the network switch level.
C. Production data is continuously replicated between primary and secondary sites.
D. Backups are maintained on multiple sites and regularly reviewed.

Answer: A

Explanation:

Question: 853

Which of the following will BEST facilitate timely and effective incident response?

A. Including penetration test results in incident response planning
B. Assessing the risk of compromised assets
C. Classifying the severity of an incident
D. Notifying stakeholders when invoking the incident response plan

Answer: C

Explanation:

Question: 854

To ensure the information security of outsourced IT services, which of the following is the MOST critical due diligence activity?

A. Request the service provider comply with information security policy.
B. Review a recent independent audit report of the service provider.
C. Assess the level of security awareness of the service provider.
D. Review samples of service level reports from the service provider.

Answer: B

Explanation:

Question: 855

An information security policy was amended recently to support an organization's new information security strategy. Which of the following should be the information security manager's NEXT step?

A. Evaluate the alignment with business strategy.
B. Review technical controls.
C. Update standards and procedures.
D. Refresh the security training program.

Answer: C

Explanation:

Question: 856

Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered the MOST significant exposure?

A. Mail relay server
B. Proxy server
C. Database server
D. Application server

Answer: C

Explanation:

Question: 857

Which of the following is the BEST way to improve an organization's ability to detect and respond to incidents?

A. Conduct a business impact analysis (BIA).
B. Conduct periodic awareness training.
C. Perform a security gap analysis.
D. Perform network penetration testing.

Answer: B

Explanation:

Question: 858

Senior management wants to thoroughly test a disaster recovery plan (DRP) for a mission-critical system. Which of the following would provide the MOST reliable results?

A. Full interruption test
B. Parallel test
C. Simulation test
D. Structured walk-through

Answer: B

Explanation:

Question: 859

Which of the following should be an information security manager's PRIMARY concern when an organization is expanding business to a new country?

A. Compliance with local regulations
B. Changes in IT infrastructure
C. Cultural differences in the new country
D. Ability to gather customer data

Answer: A

Explanation:

Question: 860

When developing security processes for handling credit card data on the business unit's information system, the information security manager should FIRST:

A. ensure alignment with industry encryption standards.
B. ensure that systems that handle credit card data are segmented.
C. review industry best practices for handling secure payments.
D. review corporate policies regarding credit card information.

Answer: D

Explanation:

Question: 861

The PRIMARY benefit of integrating information security activities into change management processes is to:

A. protect the organization from unauthorized changes.
B. ensure required controls are included in changes.
C. provide greater accountability for security-related changes in the business.
D. protect the business from collusion and compliance threats.

Answer: B

Explanation:

Question: 862

Which of the following BEST indicates misalignment of security policies with business objectives?

A. Low completion rate of employee awareness training
B. Lack of adequate funding for the security program
C. A large number of long-term policy exceptions
D. A large number of user noncompliance incidents

Answer: C

Explanation:

Question: 863

Which of the following business units should own the data that populates an identity management system?

A. Human resources (HR)
B. Legal
C. Information technology
D. Information security

Answer: A

Explanation:

Question: 864

Which of the following should be the FIRST consideration when developing a strategy for protecting an organization's data?

A. Classification

B. Encryption
C. Access monitoring
D. Access rights

Answer: A

Explanation:

Question: 865

An incident handler is preparing a forensic image of a hard drive. Which of the following MUST be done to provide evidence that the image is an exact copy of the original?

A. Perform a manual verification of file counts.
B. Encrypt and back up the hard drive before copying.
C. Use the same hardware for the image as the original.
D. Perform digital hashing of the original and the image.

Answer: D

Explanation:

Question: 866

Which of the following is the PRIMARY objective of testing security controls within a critical infrastructure?

A. Ensuring the continued resilience and security of IT services
B. Decreasing the percentage of security deployments that cause failures in production
C. Reducing the number of control assessments to optimize resources
D. Identifying and addressing security team performance issues

Answer: A

Explanation:

Question: 867

Senior management is concerned about data exposure through the use of public AI services. Which of the following is the information security manager's BEST course of action?

A. Train all employees on the appropriate use of public AI services and confidential data.
B. Disable access to public AI from company devices.
C. Perform a risk assessment of public AI with appropriate recommendations for senior management.
D. Perform a business impact analysis (BIA) of public AI.

Answer: C

Explanation:

Question: 868

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Establish performance metrics for the team
B. Perform a post-incident review
C. Implement a SIEM solution
D. Perform a threat analysis

Answer: B

Explanation:

Performing a post-incident review (also known as a lessons-learned session) is the best way to ensure similar incidents are identified and addressed more efficiently in the future. This review helps in understanding what went wrong, what went right, and how processes can be improved. The knowledge gained from the review can be incorporated into incident response plans and training. "Post-incident reviews help determine root causes, assess the effectiveness of the response, and identify opportunities for improvement."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis

Additionally, the ISACA CISM Practice Question Database emphasizes that post-incident reviews are essential for improving future response times and understanding patterns of threats.

Question: 869

Which of the following tasks would provide a newly appointed information security manager with the BEST view of the organization's existing security posture?

A. Reviewing policies and procedures
B. Performing a risk assessment
C. Interviewing business managers and employees
D. Performing a business impact analysis (BIA)

Answer: B

Explanation:

Performing a risk assessment gives a holistic and objective understanding of the threats, vulnerabilities, and controls across the organization. It reveals actual risk exposures and the effectiveness of current controls, which directly reflect the organization's security posture.

"Risk assessments identify and evaluate risk and provide the basis for determining how those risks should be

managed and mitigated."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment According to ISACA's CISM Practice Question Database, performing a risk assessment is prioritized over reviewing documents or conducting interviews because it offers direct insight into current exposures and control effectiveness.

Question: 870

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:

A. Perform a risk assessment
B. Perform a gap analysis
C. Review information security policies
D. Review the state of security awareness

Answer: A

Explanation:

During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.

"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

Question: 871

Following an unsuccessful denial of service (DoS) attack, identified weaknesses should be:

A. Tracked and reported on until their final resolution
B. Noted and re-examined later if similar weaknesses are found
C. Documented in security awareness programs
D. Quickly resolved and eliminated regardless of cost

Answer: A

Explanation:

Any weaknesses identified, even after an unsuccessful attack, should be tracked and reported until they are fully resolved. This ensures accountability, remediation, and prevention of future incidents. Ignoring or delaying action increases exposure to future threats.

"All vulnerabilities must be tracked, assigned for remediation, and closed out following proper documentation and validation."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Remediation and Lessons Learned

ISACA's guidance in the practice questions clearly recommends formal tracking and resolution of vulnerabilities as the best practice for ongoing security management.

Question: 872

Which type of policy BEST helps to ensure that all employees, contractors, and third-party users receive formal communication regarding an organization's security program?

A. Management review policy
B. Business continuity management policy
C. Information security training policy
D. Security incident management policy

Answer: C

Explanation:

The information security training policy ensures that everyone within the organization, including contractors and third-party users, receives the appropriate level of security awareness and training. This policy defines how the organization communicates its security requirements, expectations, and best practices.

"Information security training policies and programs ensure that all personnel are aware of and understand the security requirements and their individual responsibilities."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training

The ISACA CISM practice questions emphasize that a clear training policy is the best way to communicate security practices to all involved parties.

Question: 873

The PRIMARY purpose of vulnerability identification is to:

A. Remediate vulnerabilities before they are exploited
B. Discover control deficiencies
C. Provide vulnerability identifiers for risk reporting
D. Prioritize vulnerability remediation

Answer: A

Explanation:

The primary purpose of identifying vulnerabilities is to remediate them before they can be exploited by malicious actors. While risk reporting and prioritization are part of the overall process, the most immediate

goal is remediation.

"Vulnerability assessments identify weaknesses that need to be addressed to reduce risk to acceptable levels and prevent potential exploits."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis

This aligns with ISACA's official practice questions, where vulnerability identification directly aims to prevent exploitation.

Question: 874

Which of the following is the MOST critical input to developing policies, standards, and procedures to secure information assets?

A. Vulnerability assessment
B. Regulatory requirements
C. Industry best practices
D. Enterprise goals

Answer: D

Explanation:

Enterprise goals are the most critical input because security policies must align with and support the organization's objectives and mission. Policies that do not align with enterprise goals are less likely to gain management support and may not effectively protect key assets.

"Information security must support enterprise goals and objectives to ensure alignment with the broader business strategy."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Alignment with Business Goals and Objectives

ISACA's CISM questions reiterate that alignment with enterprise goals is essential for policy effectiveness.

Question: 875

The executive management of a domestic organization has announced plans to expand operations to multiple international locations. Which of the following should be the information security manager's FIRST step upon learning of these plans?

A. Perform a gap analysis against international information security standards
B. Update security training and awareness resources accordingly
C. Research legal and regulatory requirements impacting the new locations
D. Prepare localized information security policies for each new location

Answer: C

Explanation:

The first step is to research legal and regulatory requirements for the new locations. Different countries have varying security and privacy laws, and understanding these is critical before adapting policies or procedures.

"Security requirements will vary depending on local legal and regulatory obligations, which must be understood as part of international expansion."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Requirements

The ISACA CISM practice database also highlights this step as the initial and critical move in international expansions.

Question: 876

Which of the following should be the PRIMARY focus for an information security manager when reviewing access controls for data stored in an off-premise cloud environment?

A. Reviewing and updating access controls in response to changes in organizational structure
B. Implementing strong password policies and enforcing regular password changes
C. Ensuring access is granted to only those individuals whose job functions require it
D. Implementing strong encryption protocols to protect sensitive data

Answer: C

Explanation:

The principle of least privilege—ensuring access is granted only to those whose job functions require it—is the primary control for securing data, especially in cloud environments.

"Access to information and systems should be based on the principles of least privilege and need to know, regardless of environment."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Access Control Management

ISACA's CISM practice questions consistently highlight this principle as central to effective cloud security.

Question: 877

Which of the following has the GREATEST impact on the effectiveness of an organization's security posture?

A. Incident metrics are frequently compared against industry benchmarks
B. New hires are mandated to attend security training
C. Security is embedded in organizational culture
D. Senior management has approved and endorsed security practices

Answer: C

Explanation:

When security is embedded in organizational culture, it becomes a shared responsibility, increasing adherence and effectiveness.

"A security-aware culture is a key component of an effective security program because it encourages responsible behavior and supports ongoing risk management."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture

ISACA's practice questions identify security culture as the foundational element impacting the organization's entire security posture.

Question: 878

When mitigation is the chosen risk treatment, which of the following roles is responsible for effective implementation of the chosen treatment?

A. Risk owner
B. Control owner
C. Business system owner
D. Application owner

Answer: B

Explanation:

The control owner is the individual accountable for implementing and managing specific controls that mitigate risks. While the risk owner is responsible for the overall risk and decision-making, it is the control owner who ensures the selected mitigation is effectively implemented and maintained. "The control owner is responsible for ensuring that the control is properly designed, implemented, and operating effectively."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment ISACA practice questions stress this distinction: the control owner is tasked with the execution of mitigation strategies.

Question: 879

Which of the following is the GREATEST challenge when developing key risk indicators (KRIs)?

A. Limiting the number of KRIs
B. Comprehensively reporting on KRIs
C. Aggregating common KRIs
D. Linking KRIs to specific risks

Answer: D

Explanation:

The biggest challenge is linking KRIs to specific risks to ensure that they accurately measure and signal potential exposures. If KRIs aren't directly connected to real risks, they won't effectively support risk management

efforts.

"A key challenge in developing KRIs is ensuring that they are directly linked to specific risks to provide meaningful and actionable insights."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Key Risk Indicators (KRIs)*

ISACA's practice questions highlight the importance of clear linkage for effective risk measurement.

Question: 880

Which of the following is MOST appropriate for an organization to consider when defining incident classification and categorization levels?

A. Maturity of incident response activities
B. Threat environment
C. Quantity of impacted assets
D. Incident impact

Answer: D

Explanation:

Incident impact is the primary factor for classification and categorization. It ensures incidents are addressed based on their potential to disrupt the organization.

"Incident impact should be the primary factor in defining categorization levels to ensure appropriate prioritization and response."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization*

ISACA practice database stresses that focusing on impact ensures incidents receive the proper response priority.

Question: 881

Which of the following BEST enables an organization to determine what activities and changes have occurred on a system during a cybersecurity incident?

A. Computer forensics
B. Continuous log monitoring
C. Root cause analysis
D. Penetration testing

Answer: A

Explanation:

Computer forensics involves analyzing systems to reconstruct activities and identify what changes or breaches have occurred. It provides a detailed understanding of the sequence of events during an incident.
"Computer forensics provides a detailed, legally defensible analysis of system activities to reconstruct the incident and identify root causes."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Forensics and Investigations*
ISACA practice questions note that computer forensics is key for reconstructing incident activities.

Question: 882

When updating the information security policy to accommodate a new regulation, the information security manager should FIRST:

A. Review key risk indicators (KRIs)
B. Perform a gap analysis
C. Consult process owners
D. Update key performance indicators (KPIs)

Answer: B

Explanation:
A gap analysis identifies the differences between current practices and the new regulatory requirements, ensuring targeted and effective policy updates.
"Performing a gap analysis is critical to identify the areas where the current policy falls short of new regulatory requirements."
— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance*
ISACA practice questions confirm that a gap analysis is the foundational step before engaging stakeholders or updating policies.

Question: 883

Which of the following should be the MOST important consideration when reviewing an information security strategy?

A. Recent security incidents
B. New business initiatives
C. Industry security standards
D. Internal audit findings

Answer: B

Explanation:

New business initiatives are the most important consideration, as security must align with business changes to effectively protect assets and support growth.

"The security strategy must be aligned with new business initiatives to ensure it continues to protect critical assets and support enterprise goals."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment*

ISACA practice questions stress that aligning with new business initiatives ensures relevance and effectiveness.

Question: 884

From a business perspective, the GREATEST benefit of an incident response plan is that it:

A. Promotes efficiency by providing predefined response procedures
B. Improves security responsiveness to disruptive events
C. Limits the negative impact of disruptive events
D. Ensures compliance with regulatory requirements

Answer: C

Explanation:

The greatest business benefit of an incident response plan is minimizing the negative impact of disruptive incidents on operations and reputation.

"The primary business objective of an incident response plan is to minimize the impact of incidents on business operations and assets."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Objectives*

ISACA practice questions reinforce that limiting impact is the key outcome from a business perspective.

Question: 885

Which of the following should be the PRIMARY focus of an organization with immature incident detection capabilities?

A. Performing penetration testing
B. Improving user awareness
C. Installing new firewalls
D. Updating security policies

Answer: B

Explanation:

User awareness is essential for improving detection capabilities in an immature environment.
Employees are often the first line of defense and can identify suspicious activities early.
"User awareness and training can significantly improve the detection of incidents by enabling employees to recognize and report suspicious activities."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Detection and Analysis*
ISACA practice questions confirm that improving user awareness is the foundational step before deploying new technologies.

Question: 886

A new risk has been identified in a high availability system. The BEST course of action is to:

A. Perform a cost-benefit analysis for mitigating controls
B. Recommend risk acceptance to the business owner
C. Develop and implement a plan to mitigate the identified risk
D. Evaluate and prioritize the identified risk

Answer: D

Explanation:

The best first step is to evaluate and prioritize the risk to determine the appropriate treatment strategy before implementing mitigation.
"Once risks are identified, they should be evaluated and prioritized to determine the best response (mitigation, transfer, acceptance, or avoidance)."
— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment* ISACA practice questions confirm the need for evaluation and prioritization before taking further action.

Question: 887

Which of the following provides the MOST assurance that a third-party hosting provider will be able to meet availability requirements?

A. Right-to-audit clause
B. The third party's incident response plan
C. Service level agreement (SLA)
D. The third party's business continuity plan (BCP)

Answer: C

Explanation:

A Service Level Agreement (SLA) is the contractual document that specifies and guarantees the availability levels the third-party hosting provider must meet. It provides the clearest and most enforceable

commitment to availability.

"SLAs establish measurable commitments that can be monitored and enforced, providing a high level of assurance that service availability will meet business requirements."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Outsourcing and Third-Party Management*

ISACA's practice questions highlight SLAs as the most direct and reliable assurance for third-party service availability.

Question: 888

A security review identifies that confidential information on the file server has been accessed by unauthorized users in the organization. Which of the following should the information security manager do FIRST?

A. Invoke the incident response plan
B. Implement role-based access control (RBAC)
C. Remove access to the information
D. Delete the information from the file server

Answer: A

Explanation:

The first step is to invoke the incident response plan to ensure a systematic, controlled, and compliant response to the security incident.

"The incident response plan should be activated immediately to investigate, contain, and resolve incidents of unauthorized access."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Execution*

ISACA practice questions also reinforce that invoking the incident response plan is the essential first response to contain the breach.

Question: 889

Which of the following is MOST important when responding to a major security incident?

A. Contacting forensic investigators
B. Following the escalation process
C. Notifying law enforcement
D. Identifying the indicators of compromise

Answer: B

Explanation:

Following the escalation process ensures that the incident is managed in accordance with established protocols, involving the right stakeholders and prioritizing the incident appropriately.
"Following the escalation process is critical to ensure that incidents are handled appropriately and

that the right personnel are engaged at the right time."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Escalation Procedures*
ISACA practice questions highlight that proper escalation is vital to ensure incidents are managed effectively and consistently.

Question: 890

Which of the following tools would be MOST helpful to an incident response team?

A. Intrusion detection system (IDS)
B. Endpoint detection and response (EDR) solution
C. User and entity behavior analytics
D. Vulnerability scanning tools

Answer: B

Explanation:

An endpoint detection and response (EDR) solution provides advanced visibility, detection, and response capabilities at the endpoint level, which are critical for investigating and responding to incidents.
"EDR solutions help identify, investigate, and respond to threats on endpoints quickly, making them vital for incident response teams."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Tools and Technologies for Incident Response*
ISACA's practice questions highlight EDR as the most helpful tool for comprehensive incident analysis and response.

Question: 891

An information security manager is alerted to multiple security incidents across different business units, with unauthorized access to sensitive data and potential data exfiltration from critical systems. Which of the following is the BEST course of action to appropriately classify and prioritize these incidents?

A. Assemble the incident response team to evaluate the incidents
B. Initiate the crisis communication plan to notify stakeholders of the incidents
C. Engage external incident response consultants to conduct an independent investigation
D. Prioritize the incidents based on data classification standards

Answer: D

Explanation:

Prioritizing incidents based on data classification standards ensures that the most sensitive and critical data exposures are addressed first, reducing the potential impact on the business.

"The impact of incidents should be evaluated based on the classification and sensitivity of the data involved."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization*

ISACA practice questions emphasize the importance of using data classification to properly prioritize incident response efforts.

Question: 892

Which of the following is MOST important for an organization to have in place to determine the effectiveness of information security governance?

A. Program metrics
B. Key risk indicators (KRIs)
C. Risk register
D. Security strategy

Answer: A

Explanation:

Program metrics measure the effectiveness of governance processes and provide a basis for continuous improvement and informed decision-making.

"Metrics are essential for evaluating governance performance, demonstrating effectiveness, and identifying areas for improvement."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Monitoring and Metrics*

ISACA's practice questions confirm that program metrics are key to evaluating governance effectiveness.

Question: 893

A department has reported that a security control is no longer effective. Which of the following is the information security manager's BEST course of action?

A. Replace the control
B. Check for defense in depth
C. Assess the control state
D. Report the failure to management

Answer: C

Explanation:

The best first step is to assess the control state to determine why it is ineffective and whether adjustments, replacements, or compensating controls are needed.

"Regularly assess the effectiveness of security controls to ensure they are providing the intended level of protection."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Control Monitoring and Assessment*

ISACA practice questions stress that assessing the control state comes before taking further action.

Question: 894

A business continuity plan (BCP) should contain:

A. Hardware and software inventories
B. Data restoration procedures
C. Information about eradication activities
D. Criteria for activation

Answer: D

Explanation:

Criteria for activation are essential to ensure that the BCP is triggered appropriately in response to a disruption.

"The BCP should include clearly defined activation criteria to ensure that plans are invoked when necessary."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Planning*

ISACA's practice questions confirm that criteria for activation are core to a BCP's effectiveness.

Question: 895

Which of the following is MOST difficult to measure following an information security breach?

A. Reputational damage
B. Human resource costs
C. Regulatory sanctions
D. Replacement efforts

Answer: A

Explanation:

Reputational damage is often intangible, subjective, and hard to quantify, making it the most challenging aspect to measure.

"Reputation impact is difficult to quantify and may have long-term effects that are not immediately apparent."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis*

ISACA practice questions highlight that reputational damage is uniquely challenging to measure accurately.

Question: 896

Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?

A. Escalation processes
B. Technological capabilities
C. Recovery time objective (RTO)
D. Security audit reports

Answer: A

Explanation:

Escalation processes ensure that the provider and the organization can coordinate quickly and effectively during incidents.
"A clearly defined escalation process ensures that incidents are handled swiftly and with the appropriate level of authority, particularly when working with cloud service providers." — CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Cloud and Outsourced Incident Response*
ISACA practice questions reinforce that escalation processes are critical when collaborating with third parties in incident management.

Question: 897

Which of the following is MOST important to ensure incident management readiness?

A. The plan is compliant with industry standards.
B. The plan is regularly tested.
C. The plan is updated annually.
D. The plan is concise and includes a checklist.

Answer: B

Explanation:

Regular testing ensures that the incident management plan is practical and effective in real-world scenarios.

"Regular testing of the incident response plan is essential to verify that it can be executed effectively and that staff understand their roles."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Testing and Evaluation*

Question: 898

An organization is transitioning to a Zero Trust architecture. Which of the following is the information security manager's BEST approach for communicating the implications of this transition to the board of directors?

A. Present a diagram of core Zero Trust logical components to help visualize the architectural changes B. Summarize the training plan and end user feedback in an internal portal and send the link to the board
C. Prepare a report on the Zero Trust implementation that includes a status dashboard and timeline
D. Provide an outline of the business impact in terms of risk reduction and changes in user experience

Answer: D

Explanation:

Senior leadership needs to understand how Zero Trust supports risk reduction and business needs. Communicating the impact on risk reduction and user experience aligns security initiatives with business goals.

"Communicating how security initiatives support business objectives and risk reduction is critical for gaining senior management support."

E. CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment*

Question: 899

Which of the following is the PRIMARY impact of organizational culture on the effectiveness of an information security program?

A. The culture shapes behaviors toward information security.
B. The culture defines responsibilities necessary for program implementation.
C. The culture helps determine budget for information security controls.
D. The culture has minimal impact as long as information security controls are adhered to.

Answer: A

Explanation:

A culture that supports security encourages behaviors that protect information assets.

"Organizational culture has a significant impact on how employees approach security, influencing their behavior and adherence to policies."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture*

Question: 900

Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?

A. Determine the final root cause of the incident.
B. Remove all instances of the incident from the network.

C. Mitigate exploited vulnerabilities to prevent future incidents.
D. Isolate affected systems to prevent the spread of damage.

Answer: D

Explanation:

Isolating affected systems limits the damage and prevents the incident from impacting other parts of the organization.
"During containment, the primary objective is to isolate affected systems to prevent further damage."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Process*

Question: 901

An organization has identified a weakness in the ability of its employees to identify and report cybersecurity incidents. Although training materials have been provided, employees show a lack of interest. Which of the following is the information security manager's BEST course of action?

A. Block network access until security awareness training is complete.
B. Conduct an enterprise cybersecurity risk assessment.
C. Obtain key stakeholder and leadership support.
D. Send an email mandating training for the employees.

Answer: C

Explanation:

Leadership support reinforces the importance of security awareness and motivates employees to engage with training.
"Security awareness programs are most effective when they have visible support from senior management, reinforcing their importance."

— CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training*

Question: 902

A global organization is developing an incident response team. The organization wants to keep headquarters informed of all incidents and wants to be able to present a unified response to widely dispersed events. Which of the following BEST supports these objectives?

A. Virtual incident response team
B. Distributed incident response team
C. Outsourced incident response team
D. Centralized incident response team

Answer: D

Explanation:

A centralized incident response team ensures consistent communication, coordination, and a unified approach to managing incidents across the organization.

"A centralized incident response team provides a consistent and coordinated approach to incident handling and ensures that management is kept informed."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Organization Models*

Question: 903

An organization has decided to implement an Internet of Things (IoT) solution to remain competitive in the market. Which of the following should information security do FIRST?

A. Recalculate risk profile
B. Implement compensating controls
C. Reassess risk tolerance levels
D. Update the security architecture

Answer: A

Explanation:

When introducing new technologies, the first step is to recalculate the risk profile to identify any new or changed risks.

"The implementation of new technologies should trigger a review of the risk profile to identify and address new exposures."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis*

Question: 904

Which of the following provides the BEST indication of the return on information security investment?

A. Increased annualized loss expectancy (ALE)
B. Increased number of reported incidents
C. Reduced annualized loss expectancy (ALE)
D. Decreased number of reported incidents

Answer: C

Explanation:

A reduction in annualized loss expectancy (ALE) demonstrates that implemented controls have effectively

reduced the organization’s exposure to risk.

“ALE reduction is a key indicator of the cost-effectiveness of security investments and the improvement of the risk posture.”

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Cost-Benefit Analysis*

Question: 905

What should be an information security manager’s FIRST course of action upon learning a business unit is bypassing an existing control in order to increase operational efficiency?

A. Report the noncompliance to senior management.
B. Assess the risk of noncompliance.
C. Activate the incident response plan.
D. Evaluate possible compensating controls.

Answer: B

Explanation:

Assessing the risk of noncompliance ensures that decisions are based on an understanding of the business impact and security implications.

“Before reporting or remediating, it is critical to assess the risk associated with the control bypass to make informed decisions.”

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment*

Question: 906

Which of the following is the BEST strategy when determining an organization's approach to risk treatment?

A. Implementing risk mitigation controls that are considered quick wins
B. Prioritizing controls that directly mitigate the organization's most critical risks
C. Advancing the maturity of existing controls based on risk tolerance
D. Implementing a one-size-fits-all set of controls across all organizational units

Answer: B

Explanation:

Risk treatment should be prioritized based on risk criticality. Addressing the most severe and likely risks first ensures that resources are focused where they can have the greatest impact.

“Risk treatment efforts should focus on the most significant risks first, based on likelihood and impact.”

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment

Options*

Question: 907

Which of the following is the MOST effective way to influence organizational culture to align with security guidelines?

A. Adhere to regulatory requirements
B. Conduct security awareness
C. Document and distribute security procedures
D. Communicate and enforce security policies

Answer: D

Explanation:

Communicating and enforcing policies demonstrates leadership commitment and drives behavior across the organization, fostering a culture of security.
"Policies must be effectively communicated and enforced to influence culture and employee behavior."
— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Security Culture*

Question: 908

Which of the following risks is an example of risk transfer?

A. Utilizing third-party applications
B. Moving risk ownership to another department
C. Conducting off-site backups
D. Purchasing cybersecurity insurance

Answer: D

Explanation:

Purchasing cybersecurity insurance is a textbook example of risk transfer — transferring financial risk to a third party (the insurer).
"Risk transfer shifts the impact of a risk to another party, such as through insurance or outsourcing." — CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*

Question: 909

Which of the following is the MOST common cause of cybersecurity breaches?

A. Lack of adequate password rotation
B. Human error
C. Abuse of privileged accounts

D. Lack of control baselines

Answer: B

Explanation:

Human error remains the leading cause of cybersecurity breaches, including mishandling data, misconfigurations, and falling for phishing attacks.

"Human error continues to be one of the most common causes of data breaches and security incidents."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Root Cause Analysis*

Question: 910

When is the BEST time to verify that a production system's security mechanisms meet control objectives?

A. During quality and acceptance checks
B. On a continuous basis through monitoring activities and automated tooling
C. After remediations recommended by penetration tests have been completed
D. During annual internal and compliance audits

Answer: B

Explanation:

While audits and assessments provide periodic insights, the best time to verify that security mechanisms meet control objectives is continuously—through monitoring and automation. Continuous monitoring allows the organization to detect misconfigurations, anomalies, or control failures in real-time, significantly improving response capabilities. Modern environments, especially in production systems, require real-time feedback loops to maintain compliance and effectiveness due to rapidly evolving threats and configuration changes.

"Continuous monitoring provides assurance that controls are operating effectively in real time, enabling timely corrective actions."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Control Monitoring*

Question: 911

Which of the following should have the MOST influence on the development of information security policies?

A. Business strategy
B. Past and current threats
C. IT security framework
D. Industry standards

Answer: A

Explanation:

Business strategy is the overarching driver for any organizational initiative, including security. Information security policies must align with the strategic goals of the organization to ensure relevance, support, and effectiveness.

Security policies that do not consider the business context may hinder operations or fail to protect key objectives. Business-driven policies are more likely to gain executive support and compliance from stakeholders, creating a strong foundation for governance.

"Information security policies must be aligned with business goals and objectives to ensure that they support the overall mission and are embraced by stakeholders."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Strategy Alignment*

Question: 912

What is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

A. To share responsibility for addressing security breaches
B. To gain acceptance of the policy across the organization
C. To decrease the workload of the IT department
D. To reduce the overall cost of policy development

Answer: B

Explanation:

Involving stakeholders from various business units promotes buy-in, relevance, and adherence. When users feel they've had input in shaping the policy, they're more likely to support and follow it. Stakeholders also provide insights into business processes that help ensure policies are practical and tailored. This collaboration enhances organizational alignment and ensures policies do not create unintended operational friction.

"Stakeholder involvement is key to ensuring that policies are practical, aligned with operations, and accepted throughout the organization."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Policy Development and Implementation*

Question: 913

An organization is in the process of defining policies for employee use of social medi a. It is MOST important for the information security manager to:

A. Assign accountability for monitoring social media
B. Identify security monitoring tools
C. Evaluate risks to the organization
D. Develop security awareness training

Answer: C

Explanation:

Before drafting or enforcing policies, the first step is to evaluate the risks posed by employee use of social media. This may include data leakage, reputational damage, phishing, and legal liability.
Once risks are identified and understood in the organization's context, policies can be developed that specifically address those risks. Acting prematurely without a risk assessment can lead to overly restrictive or insufficient policies.
"Security policies should be risk-driven. Understanding potential threats and impacts is the foundation for effective policy creation."
— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: RiskBased Policy Development*

Question: 914

An organization requires that business-critical applications be recovered within 30 minutes in the event of a disaster. Which of the following metrics should be in the business continuity plan (BCP) to manage this requirement?

A. Maximum tolerable downtime (MTD)

B. Service level agreement (SLA)
C. Recovery point objective (RPO)
D. Recovery time objective (RTO)

Answer: D

Explanation:

The Recovery Time Objective (RTO) defines the maximum acceptable downtime for a business function or system following a disruption. If the organization requires recovery in 30 minutes, that is the system's RTO. This metric guides the selection of technologies, staffing, and procedures needed to meet recovery expectations.
"RTO defines the target time set for the recovery of IT and business activities after a disruption. It is a key BCP design parameter."
— CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery Planning*

Question: 915

Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?

A. The risks are reported to the business unit's senior management
B. The risks are escalated to the IT department for remediation
C. The risks are communicated to the central risk function

D. The risks are entered in the organization's risk register

Answer: D

Explanation:

Recording risks in the risk register ensures visibility, accountability, and tracking. This formal documentation is essential for assigning ownership, determining treatment strategies, and ensuring ongoing governance.
A risk that is not entered into the register may go unaddressed. This step supports structured risk tracking and compliance with governance practices.
"The risk register is the primary tool used to track, prioritize, assign, and monitor risks and their treatment. It forms the basis of a structured risk management program."
— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Documentation and Communication*

Question: 916

Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?

A. The risks are entered in the organization's risk register.
B. The risks are reported to the business unit's senior management.
C. The risks are escalated to the IT department for remediation.
D. The risks are communicated to the central risk function.

Answer: A

Explanation:

Entering identified risks into the organization's risk register ensures that they are documented, tracked, assigned, and addressed. Without recording in the risk register, there's no formal mechanism to manage, treat, or monitor the risk.
"The risk register is the central repository for tracking all known risks, their status, and treatment plans."
— CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Risk Response and Risk Register*

Question: 917

A new information security reporting requirement will soon become effective. Which of the following should be the information security manager's FIRST action?

A. Conduct a cost-benefit analysis related to noncompliance with the new requirement.
B. Perform a gap assessment against the new requirement.
C. Investigate to determine whether the new requirement applies to the business.
D. Inform senior management of the new requirement.

Answer: C

Explanation:

Before taking any compliance steps, the information security manager must first assess whether the regulation is applicable to the organization. This ensures resources are not spent unnecessarily. “The applicability of legal, regulatory, and contractual requirements must be determined before initiating compliance activities.”
— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Compliance*

Question: 918

Which of the following is the MOST effective way to protect the authenticity of data in transit?

A. Digital signature
B. Private key
C. Access controls
D. Public key

Answer: A

Explanation:

A digital signature validates the authenticity and integrity of a message or document. It ensures that the data was not tampered with and originated from a verified sender.
“Digital signatures provide non-repudiation and confirm both the identity of the sender and the data integrity during transmission.”
— CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Cryptographic Controls*

Question: 919

Which of the following is the MOST important reason for an information security manager to archive and retain the organization's electronic communication and email data?

A. To track personal use of electronic communication by users
B. To provide as evidence in legal proceedings when required
C. To meet the requirements of global security standards
D. To identify and scan attachments for malware

Answer: B

Explanation:

Retaining communications ensures the organization can produce evidence for litigation or regulatory

investigations, which is often a legal obligation.

"Organizations must retain electronic communications to support legal discovery, compliance audits, and investigative needs."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Requirements*

Question: 920

Which of the following is the MOST important factor in successfully implementing Zero Trust?

A. Preferring networks that have undergone penetration testing
B. Focusing on logging and monitoring of user behavior
C. Authenticating and authorizing strategic points of the architecture
D. Understanding each component of the network

Answer: C

Explanation:

Zero Trust requires granular authentication and authorization at every critical juncture. It assumes no implicit trust within the network and enforces strict access control.

"Zero Trust is based on continuous authentication and authorization at all strategic control points." — CISM Review Manual 15th Edition, Chapter 3: Security Architecture, Section: Zero Trust Principles*

Question: 921

An organization requires that business-critical applications be recovered within 30 minutes in the event of a disaster. Which of the following metrics should be defined in the business continuity plan (BCP) to manage this requirement?

A. Recovery time objective (RTO)
B. Recovery point objective (RPO)
C. Maximum tolerable downtime (MTD)
D. Service level agreement (SLA)

Answer: A

Explanation:

The Recovery Time Objective (RTO) specifies the maximum acceptable downtime before operations must resume. A 30-minute requirement directly defines the RTO for those systems.

"RTO defines the duration within which systems must be restored following an outage to prevent unacceptable business impact."

— CISM Review Manual 15th Edition, Chapter 3: Business Continuity Planning, Section: Continuity Metrics*

Question: 922

Which of the following risk responses is an example of risk transfer?

A. Utilizing third-party applications
B. Purchasing cybersecurity insurance
C. Moving risk ownership to another department
D. Conducting off-site backups

Answer: B

Explanation:

Risk transfer involves shifting the impact or financial consequences of a risk to a third party. Purchasing cybersecurity insurance is the most common example, where the organization pays a premium to a provider who assumes certain financial responsibilities in the event of a security incident.
Other options listed do not transfer risk:
A . Using third-party applications may introduce new risks, not transfer existing ones.
C . Moving ownership within the organization is reassignment, not transfer.
D . Off-site backups are a form of risk mitigation, not transfer.
"Risk transfer shifts the financial consequences of a risk to another entity, typically through insurance or contractual arrangements."
— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options*
Example: "An organization may transfer the financial impact of a potential data breach through the purchase of cyber insurance."

Question: 923

An organization has discovered that a server processing real-time visual data could be vulnerable to a lateral movement stage in a ransomware attack. Which of the following controls BEST mitigates this vulnerability?

A. Network segmentation
B. Data loss prevention (DLP)
C. Encryption of data in transit
D. Intrusion detection system (IDS)

Answer: A

Explanation:

Network segmentation is the most effective control to prevent lateral movement. In ransomware attacks, attackers often breach one endpoint and move laterally across the network to reach critical assets.
Segmentation limits this movement by isolating systems into different zones or subnets, thereby reducing the attack surface and preventing unauthorized internal traversal.
DLP and encryption are primarily focused on data protection, not internal network movement.
IDS can detect intrusions but does not prevent movement like segmentation does.

"Network segmentation limits the scope of access for compromised systems and is a key strategy in preventing lateral movement in an attack."
— CISM Review Manual 15th Edition, Chapter 3: Information Security Architecture, Section: Network Security*
Real-world example: "In the NotPetya and WannaCry incidents, poor internal segmentation allowed malware to propagate rapidly."

Question: 924

Which of the following should be of GREATEST concern regarding an organization's security controls?

A. Some controls are performing outside of an acceptable range.
B. No key control indicators (KCIs) have been implemented.
C. Control ownership has not been updated.
D. Control gap analysis is outdated.

Answer: B

Explanation:

Key Control Indicators (KCIs) are essential to measuring the effectiveness and performance of security controls. Without them:
The organization cannot assess if controls are working as intended
It's difficult to demonstrate due diligence
Risks may go unnoticed
While other answers point to operational concerns, the complete absence of KCIs presents a critical governance gap that compromises the organization's ability to monitor and manage control health. "KCIs provide actionable metrics that support proactive control management and are fundamental to governance and assurance."
— CISM Review Manual 15th Edition, Chapter 1: Governance Metrics and Reporting*

Question: 925

An organization wants to migrate a proprietary application to be hosted by a third-party cloud hosting provider using a Platform as a Service (PaaS) model. Prior to selecting the cloud provider, what is MOST important for the organization to ensure?

A. The cloud provider can meet recovery point objectives (RPOs).
B. The cloud provider adheres to applicable regulations.
C. The cloud provider's service level agreement (SLA) includes availability requirements.
D. The hosting contract has a termination clause.

Answer: B

Explanation:

When outsourcing to a cloud provider, regulatory compliance is paramount—especially with sensitive or

proprietary applications. Non-compliance could result in legal penalties, fines, or reputational damage. While RPOs, SLAs, and contract clauses are critical components of vendor risk management, ensuring adherence to relevant laws and industry regulations (such as GDPR, HIPAA, PCI DSS) is the first priority in cloud migration decisions.

"Prior to selecting a cloud provider, legal, regulatory, and contractual requirements must be reviewed to ensure alignment."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Considerations in Cloud Computing*

Question: 926

Which of the following is the PRIMARY benefit of training service desk staff to recognize incidents?

A. Incident response plan can be activated in a timely manner.
B. Incident metrics can be communicated.
C. Risk response options can be identified quickly.
D. Incident classification times can be improved.

Answer: A

Explanation:

The service desk is often the first point of contact for users. If trained properly, they can quickly recognize signs of an incident and escalate it, triggering the incident response process promptly. This early detection and escalation are essential for minimizing damage and response time. "Training frontline support staff ensures timely detection and escalation of incidents, which is critical for effective containment."

— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Roles and Responsibilities*

Question: 927

Which of the following BEST protects against emerging advanced persistent threat (APT) actors?

A. Honeypot environment
B. Updated security awareness materials
C. Ongoing incident response training
D. Proactive monitoring

Answer: D

Explanation:

Proactive monitoring (e.g., threat hunting, real-time log analysis, anomaly detection) is the most effective defense against Advanced Persistent Threats (APTs), which are stealthy, well-resourced, and long-term attacks.

APT actors:

Use zero-day exploits

Maintain long-term unauthorized access

Avoid detection

Traditional controls often fail. Proactive monitoring detects anomalies early, allowing for faster mitigation.

"Ongoing monitoring and detection programs are essential for identifying and responding to persistent and evolving threats."

— CISM Review Manual 15th Edition, Chapter 4: Threat Management, Section: APT Detection Techniques*

Question: 928

Which of the following is the MOST important consideration during the design phase of a business impact analysis (BIA)?

A. Selecting quality metrics to monitor business performance
B. Estimating the likelihood that end-to-end processes will be disrupted
C. Obtaining reserve funding to prepare for possible business failures
D. Identifying critical functions for business operations

Answer: D

Explanation:

The design phase of a BIA must begin with identifying critical business functions, since they determine:

Which systems/processes need protection

Recovery priorities

Acceptable downtime (RTO/MTD)

Without clearly defining what's critical, the BIA cannot guide resource allocation or continuity strategies effectively.

"A successful BIA must begin with identifying which business functions are critical to achieving organizational objectives."

— CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery, Section: BIA Methodology*

Question: 929

Who should be responsible for determining the level of data classification required for an application related to a new line of business?

A. Data analyst
B. Information security officer (ISO)
C. Data custodian
D. Data owners

Answer: D

Explanation:

Data owners are responsible for determining the classification of data based on its sensitivity, value, and business impact. They understand the context in which the data is used and can best evaluate its importance and risk profile.

"Data owners are responsible for defining the classification and protection requirements of their data."
— CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Data Classification Roles*

The ISO may assist in developing the classification scheme, but the final responsibility lies with the data owner.

Question: 930

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

A. Security maturity assessment results
B. Threat analysis of the organization's environment
C. Results of vulnerability assessments
D. External penetration test findings

Answer: A

Explanation:

A security maturity assessment evaluates not only current vulnerabilities but also governance structures, risk management practices, incident response, and ongoing improvement processes. It provides a holistic and strategic view of the security posture.

"Maturity assessments provide a comprehensive evaluation of an organization's security controls and their alignment with business objectives."
— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Maturity Models*

Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

Question: 931

Which of the following BEST helps to ensure a third-party backup site continues to meet the organization's information security standards?

A. Service level agreement (SLA)
B. Memorandum of understanding (MoU)
C. Business continuity plan (BCP)
D. Disaster recovery plan (DRP)

Answer: A

Explanation:

A Service Level Agreement (SLA) is a legally binding document that defines the performance and compliance expectations for third-party services, including information security requirements. It is the best mechanism to ensure that the third-party backup site meets ongoing security standards. “SLAs should include security, availability, and performance expectations to align third-party services with organizational policies.”

— CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Third-Party Relationships*

Question: 932

The department head of application development has decided to accept the risks identified in a recent assessment. No recommendations will be implemented, even though the recommendations are required by regulatory oversight. What should the information security manager do NEXT?

A. Review the risk monitoring plan.
B. Formally document the decision.
C. Review the regulations.
D. Advise the risk management team.

Answer: D

Explanation:

Since the identified risks are subject to regulatory requirements, and cannot simply be accepted without oversight, the information security manager should escalate the issue to the risk management team or higher authority to ensure proper governance.

“When risk acceptance contradicts regulatory requirements, it must be escalated to senior management or the risk function for resolution.”

— CISM Review Manual 15th Edition, Chapter 1: Governance Responsibilities, Section: Risk Governance and Oversight*

Question: 933

For an e-business that requires high availability, which of the following design principles is BEST?

A. Manual failover to the website of another e-business that meets the user's needs
B. A single point of entry allowing transactions to be received and processed quickly
C. Intelligent middleware to direct transactions from a downed system to an alternative
D. Availability of an adjacent cold site and a standby server with mirrored copies of critical data

Answer: C

Explanation:

Intelligent middleware enables dynamic rerouting and automated load balancing, which is crucial for high availability. This minimizes downtime and ensures continuity without manual intervention. “Middleware solutions can provide automated failover capabilities, improving system resilience and availability.”
— CISM Review Manual 15th Edition, Chapter 3: Program Development and Management, Section: Availability and Resilience*
Manual failover and cold sites introduce delays, which are not suitable for e-business environments requiring near-zero downtime.

Question: 934

Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?

A. Isolate affected systems to prevent the spread of damage
B. Determine the final root cause of the incident
C. Mitigate exploited vulnerabilities to prevent future incidents
D. Remove all instances of the incident from the network

Answer: A

Explanation:

The containment phase focuses on limiting the scope of the incident. Isolating affected systems immediately helps prevent propagation and further compromise.
“During the containment phase, isolating compromised systems is a key tactic to minimize further impact and enable safe recovery.”
— CISM Review Manual 15th Edition, Chapter 4: Incident Response Life Cycle, Section: Containment Strategies*

Question: 935

Which of the following is the BEST strategy when determining an organization’s approach to risk treatment?

A. Advancing the maturity of existing controls based on risk tolerance
B. Prioritizing controls that directly mitigate the organization's most critical risks
C. Implementing risk mitigation controls that are considered quick wins
D. Implementing a one-size-fits-all set of controls across all organizational units

Answer: B

Explanation:

The best strategy for risk treatment is to prioritize controls that directly mitigate the organization’s most critical risks. This aligns with a risk-based approach, where limited resources are directed toward areas with the highest business impact.

"Effective risk treatment involves prioritizing actions that address the most critical risks to the organization, considering impact and likelihood."
— CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation*
Advancing maturity or applying quick wins may help, but they are not as strategic or impactful as targeting top-priority risks.

Question: 936

An information security manager is assessing security risk associated with a cloud service provider. Which of the following is the MOST appropriate reference to consult when performing this assessment?

A. Previous provider service level agreements (SLAs)
B. Security control frameworks
C. Threat intelligence reports
D. Penetration test results from the provider

Answer: B

Explanation:

Security control frameworks (e.g., ISO/IEC 27001, NIST SP 800-53, CSA Cloud Controls Matrix) provide a structured and standardized approach to assess the security posture of cloud providers.
These frameworks ensure completeness and alignment with best practices.
"Standardized security frameworks enable consistent evaluation of third-party providers and alignment with industry-recognized security requirements."
— CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management*
Penetration test results and SLAs are useful, but only frameworks provide comprehensive coverage.

Question: 937

Which of the following is the GREATEST benefit of using AI tools in security operations?

A. Rapid detection and response to threats
B. Prioritized vulnerabilities
C. Reduced time and effort required to patch systems
D. Defined risk tolerance

Answer: A

Explanation:

AI-driven tools enable real-time analysis, anomaly detection, and automated response, drastically reducing the time to identify and respond to threats. This capability is particularly effective against advanced persistent threats (APTs) and zero-day exploits.
"AI tools enhance security operations by enabling rapid threat detection and incident response, often before traditional tools can react."
— CISM Review Manual 15th Edition, Chapter 4: Security Operations and Threat Intelligence*

Other benefits (e.g., prioritization or patching) are secondary compared to the speed and precision of AI-based threat response.

Question: 938

A global organization has outsourced security processes to a service provider by means of a global agreement. What is the MOST efficient approach to meet country-specific regulatory requirements?

A. Include binding corporate rules into the global agreement
B. Set up a governance organization for each country
C. Review the agreement for each country separately
D. Set up companion agreements for each country

Answer: A

Explanation:

Binding Corporate Rules (BCRs) are legally enforceable and approved data protection policies used to facilitate compliance across multiple jurisdictions. Incorporating BCRs into a global agreement enables the organization to efficiently manage regulatory obligations across countries.

"Binding corporate rules offer a scalable and consistent mechanism to address cross-border compliance in global outsourcing agreements."

— CISM Review Manual 15th Edition, Chapter 1: Governance, Section: Cross-Border Data Protection Considerations*

Creating separate agreements per country is inefficient and complex compared to centralized BCR-based governance.

Question: 939

An organization has implemented controls to mitigate risks resulting from identified vulnerabilities in an application. Which of the following is the BEST way to verify all weaknesses have been addressed?

A. Perform a vulnerability assessment
B. Conduct an internal audit
C. Conduct penetration testing
D. Prepare compensating controls

Answer: C

Explanation:

Penetration testing simulates real-world attacks to identify any remaining exploitable vulnerabilities after controls are implemented. It validates that mitigation has been successful from an attacker's perspective.

"Penetration testing is essential to verify the effectiveness of remediation efforts and ensure vulnerabilities can no longer be exploited."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Security Testing and Evaluation*

Vulnerability assessments and audits are valuable, but pen testing provides practical assurance.

Question: 940

A global organization is considering its geopolitical security risks. Which of the following is the information security manager's BEST approach?

A. Seek advice from environmental and physical security experts
B. Implement a third-party risk management framework
C. Implement controls that deny access from specific jurisdictions
D. Seek advice from enterprise risk and legal experts

Answer: D

Explanation:

Geopolitical risk involves complex legal, political, and compliance issues. The enterprise risk and legal teams are best positioned to provide guidance on how national laws, sanctions, and regulations impact operations and security strategies.

"In cases of geopolitical or cross-jurisdictional risk, coordination with legal and enterprise risk functions is essential for informed decision-making."

— CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Context*

Security and technical controls should follow this strategic evaluation.

Question: 941

As part of incident response activities, the BEST time to begin the recovery process is after:

A. The eradication phase has been completed
B. The incident response team has been established
C. The root cause has been determined
D. The incident manager has declared the incident

Answer: A

Explanation:

Recovery should not begin until the eradication phase is complete, meaning all malicious activity, malware, or unauthorized access has been removed. Starting recovery too early may reintroduce threats or result in re-infection.

"Recovery begins after eradication is complete, ensuring a clean environment for restoring services." — CISM Review Manual 15th Edition, Chapter 4: Incident Response Lifecycle, Section: Recovery Phase*

Question: 942

Which of the following is the MOST important objective of post-incident review activities?

A. Evidence collection

B. Continuous improvement
C. Incident triage
D. Incident documentation

Answer: B

Explanation:

The primary goal of post-incident review (PIR) is continuous improvement. After an incident has been contained, eradicated, and systems recovered, a formal review helps identify: What went wrong or could have been done better What controls failed or were missing
How the response process can be improved
The goal is not only to learn from the incident but also to enhance incident response capabilities, update plans, and prevent future occurrences.
"Post-incident reviews are a key activity for improving incident response processes. The goal is continuous improvement and prevention of repeat incidents."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-Incident Activities*
While incident documentation and evidence collection are components of the process, they are supportive to the broader strategic objective: learning and improving the overall security posture.

Question: 943

An information security team has started work to mitigate findings from a recent penetration test. Which of the following presents the GREATEST risk to the organization?

A. Some findings were reclassified to low risk after evaluation

B. Not all findings from the penetration test report were fixed
C. The penetration testing report did not contain any high-risk findings
D. Risk classification of penetration test findings was not performed

Answer: D

Explanation:

The greatest risk comes from not performing risk classification on the findings. Without classification, the organization cannot prioritize remediation efforts, allocate resources effectively, or understand the business impact of the vulnerabilities.
"Risk classification helps determine the priority for mitigating vulnerabilities and enables risk- informed decisions."
— CISM Review Manual 15th Edition, Chapter 2: Risk Assessment and Analysis*
Even if some findings are unfixed or reclassified, the lack of any classification process undermines the whole risk management effort.

Question: 944

Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?

A. Identify business requirements
B. Document disaster recovery procedures
C. Conduct a risk assessment
D. Perform a business impact analysis (BIA)

Answer: D

Explanation:

The Business Impact Analysis (BIA) is the first step in developing a disaster recovery plan because it identifies critical business processes, dependencies, and acceptable downtime.

"A BIA provides the foundation for disaster recovery planning by identifying business functions and their criticality."

— CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Disaster Recovery Planning*

Risk assessments follow the BIA and inform recovery strategies, but the BIA must come first.

Question: 945

Which of the following is the MOST important consideration when defining control objectives?

A. Senior management support
B. Risk appetite
C. Threat environment
D. Budget allocation

Answer: B

Explanation:

Risk appetite reflects how much risk the organization is willing to tolerate. It is the primary driver when defining control objectives, ensuring alignment with overall business strategy.

"Risk appetite should be used to guide the selection and design of control objectives to ensure risk is managed within acceptable boundaries."

— CISM Review Manual 15th Edition, Chapter 2: Risk Management Strategy*

Support, budget, and threats matter, but without alignment to risk appetite, controls may be misaligned.

Question: 946

Which of the following is the GREATEST benefit of classifying information security incidents?

A. Reporting capabilities
B. Improved chain of custody
C. Comprehensive documentation
D. Prioritized recovery

Answer: D

Explanation:

Incident classification helps determine severity, which allows security teams to prioritize recovery efforts. This ensures critical business functions are restored first.
"Incident classification is essential for establishing severity levels and response priorities."
— CISM Review Manual 15th Edition, Chapter 4: Incident Response Lifecycle, Section: Incident Classification*
Reporting and documentation are important, but prioritized recovery is the greatest business impact-driven benefit.

Question: 947

An information security manager learns that an existing supplier plans to begin using its recently developed generative AI technology for the same scope of service. A risk assessment was performed on the supplier three months ago with no outstanding findings. Which of the following is the BEST course of action to address the associated risk?

A. Suspend the use of the supplier until a risk assessment of the AI technology has been performed B. Report the change in risk to senior management

C. Review the results of the previous risk assessment
D. Add an indemnity clause in the contractual agreement at the renewal stage

Answer: A

Explanation:

Generative AI introduces new risks (e.g., data leakage, model poisoning). These risks were not part of the original assessment, so a fresh risk assessment must be conducted before continuing service. “When a significant change in third-party operations occurs, it necessitates a reassessment of risk before continuing operations.”
E. CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management*
This ensures security, compliance, and operational continuity.

Question: 948

Which of the following should be of GREATEST concern to an information security manager when evaluating a cloud service provider?

A. Data retention policies are not documented
B. There is no right to audit the security of the provider
C. The provider is new to the market and lacks references
D. Security controls offered by the provider are inadequate

Answer: B

Explanation:

The lack of audit rights prevents the organization from verifying the security posture and compliance of the provider, representing a major governance and assurance gap.
"Right to audit clauses ensure that organizations retain oversight and can verify the security controls and compliance of their service providers."
— CISM Review Manual 15th Edition, Chapter 3: Outsourced Services, Section: Third-Party Governance*
Control inadequacy can be fixed; lack of oversight cannot be tolerated.

Question: 949

Which of the following is the BEST way to evaluate the effectiveness of physical and environmental security controls implemented for fire-related disasters?

A. Conduct evacuation exercises
B. Review the disaster recovery plan (DRP)
C. Conduct awareness sessions
D. Review emergency management team procedures

Answer: A

Explanation:

Evacuation drills provide real-time validation of physical security measures, staff preparedness, and response time during fire-related scenarios. They test both people and systems.
"Simulated exercises are the most effective method to evaluate real-world preparedness and the adequacy of response procedures."
— CISM Review Manual 15th Edition, Chapter 3: Security Controls Testing*
Paper reviews and awareness are useful, but only exercises reveal actual gaps in preparedness.

Question: 950

Which of the following is the BEST course of action after management has reviewed an identified risk and determines the risk is below the defined risk appetite?

A. Accept
B. Avoid
C. Transfer

D. Mitigate

Answer: A

Explanation:

When a risk is determined to be below the organization's risk appetite, the most appropriate course of action is to formally accept the risk. Risk acceptance is a valid and cost-effective strategy when the impact and likelihood are within acceptable limits, and the cost of mitigation outweighs the potential loss.

"Risk acceptance is an appropriate response when the level of residual risk is within the organization's defined risk tolerance and appetite."

— CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation*

Avoidance, transfer, or mitigation may be overreactions that waste resources in this context.

Question: 951

The PRIMARY goal when conducting post-incident reviews is to identify:

A. Additional cybersecurity budget needs
B. Weaknesses in incident response plans
C. Information to be shared with senior management
D. Individuals that need additional training

Answer: B

Explanation:

The core objective of a post-incident review (PIR) is to identify gaps and weaknesses in the response process. This includes missteps, delays, communication failures, or policy limitations — all of which provide insight to improve future incident handling.

"Post-incident reviews focus on identifying root causes and areas for improvement to enhance the organization's preparedness for future incidents."

— CISM Review Manual 15th Edition, Chapter 4: Post-Incident Activities*

Though training, reporting, and budgeting may follow, they are secondary outcomes of this process.

Question: 952

The PRIMARY purpose for conducting cybersecurity risk assessments is to:

A. Assist in security reporting to senior management
B. Provide metrics to indicate cybersecurity program effectiveness
C. Verify compliance across multiple sectors
D. Understand the organization's current security posture

Answer: D

Explanation:

The main goal of a cybersecurity risk assessment is to gain visibility into the organization's current security posture, identify vulnerabilities, evaluate threats, and understand the potential impact of various risks.
"Risk assessments provide an understanding of the organization's threat landscape, asset vulnerabilities, and residual risk exposure."
— CISM Review Manual 15th Edition, Chapter 2: Risk Assessment and Risk Identification*
While assessments support reporting and compliance, their primary role is situational awareness.

Question: 953

Which type of system is MOST effective for monitoring cyber incidents based on impact and tracking them until they are closed?

A. Endpoint detection and response (EDR)
B. Network intrusion detection system (NIDS)
C. Extended detection and response (XDR)
D. Security information and event management (SIEM)

Answer: D

Explanation:

SIEM systems collect and analyze log data from across the organization, allowing for real-time monitoring, incident correlation, and end-to-end tracking of response activities — including severity classification and closure.
"SIEM tools enable centralized management, prioritization, and documentation of incidents, making them essential for impact tracking and incident lifecycle management."
— CISM Review Manual 15th Edition, Chapter 4: Incident Management Systems*
While EDR and XDR help detect threats, SIEMs offer the full scope for impact-based tracking.

Question: 954

An organization plans to implement a new e-commerce operation in a highly regulated market. Which of the following is MOST important to consider when updating the risk management strategy?

A. Strategy of industry peers
B. Outsourcing needs
C. Business culture
D. Compliance requirements

Answer: D

Explanation:

When operating in a highly regulated market, compliance requirements become paramount, as failure to comply can lead to severe legal penalties, financial losses, and reputational harm. According to the CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Task 2, understanding and addressing legal, regulatory, and contractual requirements is critical in risk management, especially in regulated environments. This ensures that the risk management strategy is aligned with mandatory regulations and industry standards. Other factors (such as outsourcing and business culture) are important, but compliance is the primary driver in highly regulated markets. Reference:ISACA CISM Review Manual, 16th Edition, Page 120-122, "Legal, Regulatory and Contractual Requirements".

Question: 955

Which of the following is MOST likely to reduce the effectiveness of a SIEM system?

A. Complex user interface
B. Misconfiguration of alert thresholds
C. Weakly encrypted log files
D. Lack of multi-factor authentication (MFA) for system access

Answer: B

Explanation:

The effectiveness of a SIEM (Security Information and Event Management) system heavily relies on properly configured alert thresholds. Misconfiguration of alert thresholds can result in missed detection of significant incidents (false negatives) or an overwhelming number of false positives, making it difficult to identify real threats. According to the CISM Review Manual, 16th Edition, Domain 4: Information Security Incident Management, the configuration and tuning of monitoring tools like SIEMs are crucial for timely and accurate detection of incidents.

Reference:ISACA CISM Review Manual, 16th Edition, Page 304-305, "Security Event Management Tools and Techniques".

Question: 956

Which of the following has the GREATEST impact on the ability to successfully execute a disaster recovery plan (DRP)?

A. Conducting tabletop exercises of the plan
B. Updating the plan periodically
C. Communicating the plan to all stakeholders
D. Reviewing escalation procedures

Answer: C

Explanation:

The CISM Review Manual emphasizes that the success of a DRP (Disaster Recovery Plan) depends greatly on clear communication of the plan to all stakeholders. Stakeholders must be aware of their roles and responsibilities during an incident to ensure the plan can be effectively executed. While testing, updating, and reviewing the plan are also important, communication is critical to effective execution.

Reference:ISACA CISM Review Manual, 16th Edition, Page 250-251, "Disaster Recovery Planning – Key Success Factors".

Question: 957

When defining a security baseline, it is MOST important that the baseline:

A. can vary depending on the security classification of systems.
B. is uniform for all assets of the same type.
C. is developed based on stakeholder consensus.
D. aligns to key risk indicators (KRIs).

Answer: B

Explanation:

A security baseline is a set of minimum security requirements for a system or asset type. The CISM Review Manual states that a baseline should be uniform for all assets of the same type to ensure consistency, enforceability, and ease of monitoring. This standardization supports effective compliance and security operations. While other factors can influence baseline adjustments, uniformity for similar asset types is most critical.

Reference:ISACA CISM Review Manual, 16th Edition, Page 207, "Establishing Security Baselines".

Question: 958

A department has reported that a security control is no longer effective. Which of the following is the information security manager's BEST course of action?

A. Assess the control state.
B. Replace the control.
C. Report the failure to management.
D. Check for defense in depth.

Answer: A

Explanation:

Upon learning a control is ineffective, the first action should be to assess the state of the control to verify the issue, determine its root cause, and assess the risk exposure. The CISM Review Manual emphasizes that assessment comes before taking further steps like replacement or escalation, as it informs appropriate, risk-based action.

Reference:ISACA CISM Review Manual, 16th Edition, Page 131-132, "Control Assessment and Continuous Improvement".

Question: 959

Which of the following is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

A. To reduce the overall cost of policy development
B. To share responsibility for addressing security breaches
C. To decrease the workload of the IT department
D. To gain acceptance of the policy across the organization

Answer: D

Explanation:

The main reason to involve stakeholders from various business units is to gain their acceptance and buy-in for the information security policy. The CISM Review Manual underlines that policies are more

effective and enforceable when stakeholders understand and agree with them, which also aids in smooth policy implementation across the organization.

Reference:ISACA CISM Review Manual, 16th Edition, Page 45, "Stakeholder Involvement in Policy Development".

Question: 960

Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?

A. Conduct a risk assessment.
B. Document disaster recovery procedures.
C. Identify business requirements.
D. Perform a business impact analysis (BIA).

Answer: D

Explanation:

The business impact analysis (BIA) is the foundational step in disaster recovery planning. The CISM Review Manual states that BIA should be performed first to determine critical business functions, recovery priorities,

and the impact of disruptions. Risk assessments and documentation follow after the BIA.

Reference:ISACA CISM Review Manual, 16th Edition, Page 237-238, "Business Impact Analysis (BIA) in DRP Development".

Question: 961

An information security manager is updating the organization's incident response plan. Which of the following is the BEST way to validate that the process and procedures provided by IT and business units are complete, accurate, and known by all responsible teams?

A. Review the test objectives with stakeholders.
B. Conduct a data breach incident tabletop exercise.
C. Conduct an incident response plan survey.
D. Review data breach incident triage steps.

Answer: B

Explanation:

Conducting a tabletop exercise is the best method to validate the completeness, accuracy, and awareness of incident response procedures. The CISM Review Manual details that tabletop exercises simulate scenarios, allowing teams to test responses, clarify responsibilities, and reveal gaps in the process in a controlled environment.

Reference:ISACA CISM Review Manual, 16th Edition, Page 295, "Testing and Validating Incident Response Plans".

Question: 962

Which of the following should be an information security manager's FIRST course of action when a potential business breach is discovered in a critical business system?

A. Implement mitigating actions immediately.
B. Invoke the incident response plan.
C. Inform senior management of the breach.
D. Validate the breach.

Answer: D

Explanation:

The first step when a potential breach is discovered is to validate the breach. According to the CISM Review Manual, Domain 4, the information security manager must confirm the event to avoid unnecessary escalation or resource allocation. This validation ensures that the incident is real and justifies further response actions. Invoking the incident response plan or informing management comes after the breach is validated.

Reference:ISACA CISM Review Manual, 16th Edition, Page 280, "Incident Detection and Validation".

Question: 963

The BEST way to integrate information security governance with corporate governance is to ensure:

A. the information security steering committee monitors compliance with security policies.
B. management teams embed information security into business processes.
C. awareness programs include industry best practice for information security governance.
D. the information security program is included in regular external audits.

Answer: B

Explanation:

The best way to integrate information security governance with corporate governance is for management teams to embed information security into business processes. The CISM Review Manual explains that aligning security objectives and activities with organizational goals and business processes ensures that security is a core part of business operations and strategy, not an isolated activity.
Reference:ISACA CISM Review Manual, 16th Edition, Page 38-39, "Integration of Information Security with Business Processes".

Question: 964

Which type of system is MOST effective for prioritizing cyber incidents based on impact and tracking them until they are closed?

A. Security information and event management (SIEM)
B. Extended detection and response (XDR)
C. Endpoint detection and response (EDR)
D. Network intrusion detection system (NIDS)

Answer: A

Explanation:

A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, "SIEM and Incident Prioritization".

Question: 965

An organization has an ongoing security awareness training program. Employee participation has been

decreasing over the year, while the number of malware and phishing incidents from email has been increasing. What is the information security manager's BEST course of action?

A. Report the findings to senior management with recommendations.
B. Implement a phishing reporting tool in the email system.
C. Include regular phishing campaigns after each training session.
D. Make the training program mandatory for all employees.

Answer: D

Explanation:

If participation in security awareness training is decreasing while incidents are rising, making the training program mandatory for all employees is the best course of action. The CISM Review Manual notes that mandatory training ensures organizational-wide coverage and directly addresses the lack of participation, which is likely contributing to increased incidents.
Reference:ISACA CISM Review Manual, 16th Edition, Page 220-221, "Awareness and Training – Ensuring Coverage".

Question: 966

Which of the following would be the BEST way to reduce the risk of disruption resulting from an emergency system change?

A. Confirm the change implementation is scheduled.
B. Verify the change request has been approved.
C. Confirm rollback plans are in place.
D. Notify users affected by the change.

Answer: C

Explanation:

The best way to reduce the risk of disruption from an emergency system change is to confirm rollback plans are in place. According to the CISM Review Manual, having an effective rollback (or backout) plan ensures that if the emergency change causes unexpected issues, the organization can quickly revert to a known, stable state. This minimizes downtime and impact to business operations. Approval and communication are important, but only a rollback plan directly addresses risk reduction during unexpected disruptions.
Reference:ISACA CISM Review Manual, 16th Edition, Page 210, "Change Management – Rollback Planning".

Question: 967

An organization has implemented controls to mitigate risks resulting from identified vulnerabilities in an application. Which of the following is the BEST way to verify all weaknesses have been addressed?

A. Conduct an internal audit.
B. Conduct penetration testing.
C. Perform a vulnerability assessment.
D. Prepare compensating controls.

Answer: C

Explanation:

After implementing controls, performing a vulnerability assessment is the best way to verify that all previously identified weaknesses have been addressed. The CISM Review Manual specifies that vulnerability assessments systematically scan for known vulnerabilities and confirm remediation effectiveness. Penetration testing is valuable but is typically used to exploit vulnerabilities, not comprehensively verify their remediation as efficiently as vulnerability assessments.

Reference:ISACA CISM Review Manual, 16th Edition, Page 164-165, "Vulnerability Management and Assessment".