"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."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which of the following should be an assurance requirement when an organization is migrating to a Software as a Service (SaaS) provider?

A. Location of data
B. Amount of server storage
C. Access controls
D. Type of network technology

Answer: C

Explanation:
Access controls are an assurance requirement when an organization is migrating to a SaaS provider because they ensure that only authorized users can access the cloud services and data. Access controls also help to protect the confidentiality, integrity and availability of the cloud resources. Access controls are part of the Cloud Control Matrix (CCM) domain IAM-01: Identity and Access Management Policy and Procedures, which states that "The organization should have a policy and procedures to manage user identities and access to cloud services and data."1 Reference := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 751

Question: 2

In a multi-level supply chain structure where cloud service provider A relies on other sub cloud services, the provider should ensure that any compliance requirements relevant to the provider are:

A. passed to the sub cloud service providers based on the sub cloud service providers' geographic location.
B. passed to the sub cloud service providers.
C. treated as confidential information and withheld from all sub cloud service providers.
D. treated as sensitive information and withheld from certain sub cloud service providers.

Answer: A

Explanation:
In a multi-level supply chain structure, the cloud service provider should ensure that any compliance requirements relevant to the provider are passed to the sub cloud service providers, regardless of

their geographic location. This is because the sub cloud service providers may have access to or process the data of the provider's customers, and thus may affect the compliance status of the provider. The provider should also monitor and verify the compliance of the sub cloud service providers on a regular basis. This is part of the Cloud Control Matrix (CCM) domain COM-01: Regulatory Frameworks, which states that "The organization should identify and comply with applicable regulatory frameworks, contractual obligations, and industry standards."1 Reference := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 51

Question: 3

Which of the following is the PRIMARY component to determine the success or failure of an organization's cloud compliance program?

A. Defining the metrics and indicators to monitor the implementation of the compliance program
B. Determining the risk treatment options to be used in the compliance program
C. Mapping who possesses the information and data that should drive the compliance goals
D. Selecting the external frameworks that will be used as reference

Answer: C

Explanation:

The primary component to determine the success or failure of an organization's cloud compliance program is mapping who possesses the information and data that should drive the compliance goals. This is because the cloud compliance program should be aligned with the organization's business objectives and risk appetite, and the information and data that support these objectives and risks are often distributed across different cloud service providers, business units, and stakeholders.

Therefore, it is essential to identify who owns, controls, and accesses the information and data, and how they are protected, processed, and shared in the cloud environment. This is part of the Cloud Control Matrix (CCM) domain COM-02: Data Governance, which states that "The organization should have a policy and procedures to manage data throughout its lifecycle in accordance with regulatory requirements, contractual obligations, and industry standards."1 Reference := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 53

Question: 4

Organizations maintain mappings between the different control frameworks they adopt to:

A. help identify controls with common assessment status.
B. avoid duplication of work when assessing compliance, C. help identify controls with different assessment status.
D. start a compliance assessment using the latest assessment.

Answer: B

Explanation:

Organizations maintain mappings between the different control frameworks they adopt to avoid duplication of work when assessing compliance. This is because different control frameworks may

have overlapping or equivalent controls that address the same objectives or risks. By mapping these controls, organizations can streamline their compliance assessment process and reduce the cost and effort involved. Mappings also help organizations to identify any gaps or inconsistencies in their control coverage and address them accordingly. This is part of the Cloud Control Matrix (CCM) domain COM-03: Control Frameworks, which states that "The organization should identify and adopt applicable control frameworks, standards, and best practices to support the cloud compliance program."1 Reference := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 54

Question: 5

To assist an organization with planning a cloud migration strategy to execution, an auditor should recommend the use of:

A. enterprise architecture (EA).
B. object-oriented architecture.
C. service-oriented architecture.
D. software architecture

Answer: A

Explanation:
To assist an organization with planning a cloud migration strategy to execution, an auditor should recommend the use of enterprise architecture (EA). EA is a holistic approach to aligning the business and IT objectives, processes, and resources of an organization. EA helps to define the current and future state of the organization, identify the gaps and opportunities, and design the roadmap and governance for the cloud migration. EA also helps to ensure that the cloud migration is consistent with the organization's vision, mission, values, and strategy, and that it meets the requirements of the stakeholders, customers, and regulators. EA is part of the Cloud Control Matrix (CCM) domain GRC-01: Enterprise Risk Management, which states that "The organization should have a policy and procedures to identify, assess, manage, and monitor risks related to cloud services."1 Reference := CCAK Study Guide, Chapter 2: Cloud Governance, page 25

Question: 6

The CSA STAR Certification is based on criteria outlined the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to:

A. ISO/IEC 27001 implementation.
B. GB/T 22080-2008.
C. SOC 2 Type 1 or 2 reports.
D. GDPR CoC certification.

Answer: A

Explanation:
The CSA STAR Certification is based on criteria outlined in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to ISO/IEC 27001 implementation. ISO/IEC 27001 is an international standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). The CSA STAR Certification is a third-party independent assessment of the security of a cloud service provider, which demonstrates the alignment of the provider's ISMS with the CCM best practices. The CSA STAR Certification has three levels: Level 1 (STAR Certification), Level 2 (STAR Attestation), and Level 3 (STAR Continuous Monitoring).1 [2][2] Reference := CCAK Study Guide, Chapter 5: Cloud Auditing, page 971; CSA STAR Certification, Overview[2][2]

Question: 7

What does “The Egregious 11" refer to?

A. The OWASP Top 10 adapted to cloud computing
B. A list of top shortcomings of cloud computing
C. A list of top breaches in cloud computing
D. A list of top threats to cloud computing

Answer: D

Explanation:
The Egregious 11 refers to a list of top threats to cloud computing, as published by the Cloud Security Alliance (CSA) in 2019. The CSA is a leading organization dedicated to defining standards, certifications and best practices to help ensure a secure cloud computing environment. The Egregious 11 report ranks the most critical and pressing cloud security issues, such as data breaches, misconfigurations, insufficient identity and access management, and account hijacking. The report also provides recommendations for security, compliance, risk and technology practitioners to mitigate these threats. The Egregious 11 is based on a survey of industry experts and a review of current literature and media reports. The report is intended to raise awareness of the risks and challenges associated with cloud computing and promote strong security practices.12 Reference := CCAK Study Guide, Chapter 5: Cloud Auditing, page 961; CSA Top Threats to Cloud Computing: Egregious 11

Question: 8

Which objective is MOST appropriate to measure the effectiveness of password policy?

A. The number of related incidents decreases.
B. Attempts to log with weak credentials increases.
C. The number of related incidents increases.
D. Newly created account credentials satisfy requirements.

Answer: D

Explanation:
The objective that is most appropriate to measure the effectiveness of password policy is newly created account credentials satisfy requirements. This is because password policy is a set of rules and guidelines that define the characteristics and usage of passwords in a system or network. Password policy aims to enhance the security and confidentiality of the system or network by preventing unauthorized access, data breaches, and identity theft. Therefore, the best way to evaluate the effectiveness of password policy is to check whether the newly created account credentials meet the requirements of the policy, such as length, complexity, expiration, and history. This objective can be measured by conducting periodic audits, reviews, or tests of the account creation process and verifying that the passwords comply with the policy standards. This is part of the Cloud Control Matrix (CCM) domain IAM-02: User ID Credentials, which states that "The organization should have a policy and procedures to manage user ID credentials for cloud services and data."1 Reference := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 76

Question: 9

An auditor wants to get information about the operating effectiveness of controls addressing privacy, availability, and confidentiality of a service organization. Which of the following can BEST help to gain the required information?

A. ISAE 3402 report
B. ISO/IEC 27001 certification
C. SOC1 Type 1 report
D. SOC2 Type 2 report

Answer: D

Explanation:
A SOC2 Type 2 report can best help an auditor to get information about the operating effectiveness of controls addressing privacy, availability, and confidentiality of a service organization. A SOC2 Type 2 report is an internal control report that examines the security, availability, processing integrity, confidentiality, and privacy of a service organization's system and data over a specified period of time, typically 3-12 months. A SOC2 Type 2 report is based on the AICPA Trust Services Criteria and provides an independent auditor's opinion on the design and operating effectiveness of the service organization's controls. A SOC2 Type 2 report can help an auditor to assess the risks and challenges associated with outsourcing services to a cloud provider and to verify that the provider meets the relevant compliance requirements and industry standards.12 Reference := CCAK Study Guide, Chapter 5: Cloud Auditing, page 971; SOC 2 Type II Compliance: Definition, Requirements, and Why You Need It2

Question: 10

Which of the following is a cloud-specific security standard?

A. 15027017
B. 15014001
C. 15022301
D. 15027701

Answer: A

Explanation:
ISO/IEC 15027017 is a cloud-specific security standard that provides guidelines for information security controls applicable to the provision and use of cloud services. It is based on ISO/IEC 27002, which is a general standard for information security management, but it also includes additional controls and implementation guidance that specifically relate to cloud services. ISO/IEC 15027017 is intended to help both cloud service providers and cloud service customers to enhance the security and confidentiality of their cloud environment and to comply with relevant regulatory requirements and industry standards.12 Reference := ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services1; Cloud Security Standards: ISO, PCI, GDPR and Your Cloud - Exabeam3; ISO/IEC 27017 - Wikipedia2

Question: 11

Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include:

A. regulatory guidelines impacting the cloud customer.
B. audits, assessments, and independent verification of compliance certifications with agreement terms.
C. the organizational chart of the provider.
D. policies and procedures of the cloud customer

Answer: B

Explanation:

Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include audits, assessments, and independent verification of compliance certifications with agreement terms. This is because cloud services involve multiple parties in the supply chain, such as cloud providers, sub-providers, brokers, carriers, and auditors. Each party may have different roles and responsibilities in delivering the cloud services and ensuring their quality, security, and compliance. Therefore, it is important for the cloud customers to have visibility and assurance of the performance and compliance of the cloud providers and their sub-providers. Audits, assessments, and independent verification of compliance certifications are methods to evaluate the effectiveness of the controls and processes implemented by the cloud providers and their sub-providers to meet the agreement terms. These methods can help the cloud customers to identify any gaps or risks in the supply chain and to take corrective actions if needed. This is part of the Cloud Control Matrix (CCM) domain COM-04: Audit Assurance & Compliance, which states that "The organization should have a policy and procedures to conduct audits and assessments of cloud services and data to verify compliance with applicable regulatory frameworks, contractual obligations, and industry standards."12 Reference := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 551; Practical Guide to Cloud Service Agreements Version 2.02

Question: 12

Which of the following is the reason for designing the Consensus Assessments Initiative Questionnaire (CAIQ)?

A. Cloud service providers need the CAIQ to improve quality of customer service.
B. Cloud service providers can document their security and compliance controls.
C. Cloud service providers can document roles and responsibilities for cloud security.
D. Cloud users can use CAIQ to sign statement of work (SOW) with cloud access security

Answer: B

Explanation:

The reason for designing the Consensus Assessments Initiative Questionnaire (CAIQ) is to enable cloud service providers to document their security and compliance controls in a standardized and transparent way. The CAIQ is a set of yes/no questions that correspond to the controls of the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), which is a framework of best practices for cloud security. The CAIQ helps cloud service providers to demonstrate their adherence to the CCM and to provide evidence of their security posture to potential customers, auditors, and regulators. The CAIQ also helps cloud customers and auditors to assess the security

capabilities of cloud service providers and to compare different providers based on their responses. The CAIQ is part of the CSA STAR program, which is a cloud security assurance program that offers various levels of certification and attestation for cloud service providers.12 Reference := What is CAIQ? | CSA - Cloud Security Alliance3; Consensus Assessment Initiative Questionnaire (CAIQ) v3.1 [No | CSA4

Question: 13

An organization employing the Cloud Controls Matrix (CCM) to perform a compliance assessment leverages the Scope Applicability direct mapping to:

A. obtain the ISO/IEC 27001 certification from an accredited certification body (CB) following the ISO/IEC 17021-1 standard.

B. determine whether the organization can be considered fully compliant with the mapped standards because of the implementation of every CCM Control Specification.

C. understand which controls encompassed by the CCM may already be partially or fully implemented because of the compliance with other standards.

Answer: C

Explanation:

An organization employing the Cloud Controls Matrix (CCM) to perform a compliance assessment leverages the Scope Applicability direct mapping to understand which controls encompassed by the CCM may already be partially or fully implemented because of the compliance with other standards. The Scope Applicability direct mapping is a worksheet within the CCM that maps the CCM control specifications to several standards within the ISO/IEC 27000 series, such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, and ISO/IEC 27018. The mapping helps the organization to identify the commonalities and differences between the CCM and the ISO/IEC standards, and to determine the level of compliance with each standard based on the implementation of the CCM controls. The mapping also helps the organization to avoid duplication of work and to streamline the compliance assessment process.12 Reference := What you need to know: Transitioning CSA STAR for Cloud Controls Matrix ...1; Cloud Controls Matrix (CCM) - CSA3

Question: 14

Which of the following are the three MAIN phases of the Cloud Controls Matrix (CCM) mapping methodology?

A. Initiation — Execution — Monitoring and Controlling

B. Plan - Develop - Release

C. Preparation — Execution - Peer Review and Publication

Answer: C

Explanation:

The three main phases of the Cloud Controls Matrix (CCM) mapping methodology are preparation, execution, and peer review and publication. The CCM mapping methodology is a process to map the CCM controls to other standards, regulations, or frameworks that are relevant for cloud security. The mapping helps to identify the commonalities and differences between the CCM and the other standards, regulations, or frameworks, and to provide guidance for cloud service providers and customers on how to achieve compliance with multiple

requirements using the CCM. The mapping methodology consists of the following phases1:
Preparation: This phase involves defining the scope, objectives, and deliverables of the mapping project, as well as identifying the stakeholders, resources, and tools needed. This phase also includes conducting a preliminary analysis of the CCM and the other standard, regulation, or framework to be mapped, and establishing the mapping criteria and rules.
Execution: This phase involves performing the actual mapping of the CCM controls to the other standard, regulation, or framework using a spreadsheet template. This phase also includes documenting the mapping results, providing explanations and justifications for each mapping decision, and resolving any issues or conflicts that may arise during the mapping process.
Peer Review and Publication: This phase involves validating and verifying the quality and accuracy of the mapping results by conducting a peer review with subject matter experts from both the CCM working group and the other standard, regulation, or framework organization. This phase also includes finalizing and publishing the mapping document as a CSA artifact, and communicating and promoting the mapping to the relevant audiences.
Reference := Methodology for the Mapping of the Cloud Controls Matrix1

Question: 15

When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?

A. Determine the impact on confidentiality, integrity, and availability of the information system.
B. Determine the impact on the physical and environmental security of the organization, excluding informational assets.
C. Determine the impact on the controls that were selected by the organization to respond to identified risks.
D. Determine the impact on the financial, operational, compliance, and reputation of the organization.

Answer: A

Explanation:
When applying the Top Threats Analysis methodology following an incident, the scope of the technical impact identification step is to determine the impact on confidentiality, integrity, and availability of the information system. The Top Threats Analysis methodology is a process developed by the Cloud Security Alliance (CSA) to help organizations identify, analyze, and mitigate the top threats to cloud computing, as defined in the CSA Top Threats reports. The methodology consists of six steps1:
Scope definition: Define the scope of the analysis, such as the cloud service model, deployment model, and business context.
Threat identification: Identify the relevant threats from the CSA Top Threats reports that may affect the scope of the analysis.
Technical impact identification: Determine the impact on confidentiality, integrity, and availability of the information system caused by each threat. Confidentiality refers to the protection of data from unauthorized access or disclosure. Integrity refers to the protection of data from unauthorized modification or deletion. Availability refers to the protection of data and services from disruption or denial.
Business impact identification: Determine the impact on the business objectives and operations caused by each threat, such as financial loss, reputational damage, legal liability, or regulatory compliance.
Risk assessment: Assess the likelihood and severity of each threat based on the technical and business impacts, and prioritize the threats according to their risk level.

Risk treatment: Select and implement appropriate risk treatment options for each threat, such as avoidance, mitigation, transfer, or acceptance.
The technical impact identification step is important because it helps to measure the extent of damage or harm that each threat can cause to the information system and its components. This step also helps to align the technical impacts with the business impacts and to support the risk assessment and treatment steps.
Reference := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 81

Question: 16

Which of the following is an example of availability technical impact?

A. The cloud provider reports a breach of customer personal data from an unsecured server.
B. A hacker using a stolen administrator identity alters the discount percentage in the product database.
C. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours.
D. An administrator inadvertently clicked on phish bait, exposing the company to a ransomware attack

Answer: C

Explanation:
A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours is an example of availability technical impact. Availability is the protection of data and services from disruption or denial, and it is one of the three dimensions of information security, along with confidentiality and integrity. Availability technical impact refers to the extent of damage or harm that a threat can cause to the availability of the information system and its components, such as servers, networks, applications, and data. A DDoS attack is a malicious attempt to overwhelm a target system with a large volume of traffic or requests from multiple sources, making it unable to respond to legitimate requests or perform its normal functions. A DDoS attack can cause a significant availability technical impact by rendering the customer's cloud inaccessible for a prolonged period of time, resulting in loss of productivity, revenue, customer satisfaction, and reputation.
Reference := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 81;
What is a DDoS Attack? | Cloudflare

Question: 17

Which of the following is an example of financial business impact?

A. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours, resulting in millions in lost sales.
B. A hacker using a stolen administrator identity brings down the Software of a Service (SaaS) sales and marketing systems, resulting in the inability to process customer orders or manage customer relationships.
C. While the breach was reported in a timely manner to the CEO, the CFO and CISO blamed each other in public, resulting in a loss of public confidence that led the board to replace all

Answer: A

Explanation:
A DDoS attack renders the customer's cloud inaccessible for 24 hours, resulting in millions in lost sales is an example of financial business impact. Financial business impact refers to the extent of damage or harm that a threat can cause to the financial objectives and performance of the organization, such as revenue, profit, cash flow, or market share. A DDoS attack can cause a significant financial business impact by disrupting the normal

operations and transactions of the organization, leading to loss of sales, customers, contracts, or opportunities. According to a report by Kaspersky, the average cost of a DDoS attack for small and medium-sized businesses (SMBs) was $123,000 in 2019, while for enterprises it was $2.3 million.1 Therefore, it is important for organizations to implement appropriate security measures and contingency plans to prevent or mitigate the effects of a DDoS attack. Reference := The Future of Finance and the Global Economy: Facing Global ... - IMF2; Kaspersky: Cost of a DDoS Attack1

Question: 18

After finding a vulnerability in an Internet-facing server of an organization, a cybersecurity criminal is able to access an encrypted file system and successfully manages to overwrite parts of some files with random dat a. In reference to the Top Threats Analysis methodology, how would the technical impact of this

incident be categorized?

A. As an availability breach
B. As a control breach
C. As a confidentiality breach
D. As an integrity breach

Answer: D

Explanation:

The technical impact of this incident would be categorized as an integrity breach in reference to the Top Threats Analysis methodology. The Top Threats Analysis methodology is a process developed by the Cloud Security Alliance (CSA) to help organizations identify, analyze, and mitigate the top threats to cloud computing, as defined in the CSA Top Threats reports. The methodology consists of six steps: scope definition, threat identification, technical impact identification, business impact identification, risk assessment, and risk treatment. Each of these provides different insights and visibility into the organization's security posture.1

The technical impact identification step involves determining the impact on confidentiality, integrity, and availability of the information system caused by each threat. Confidentiality refers to the protection of data from unauthorized access or disclosure. Integrity refers to the protection of data from unauthorized modification or deletion. Availability refers to the protection of data and services from disruption or denial.2

An integrity breach occurs when a threat compromises the accuracy and consistency of the data or system. An integrity breach can result in data corruption, falsification, or manipulation, which can affect the reliability and trustworthiness of the data or system. An integrity breach can also have serious consequences for the business operations and decisions that depend on the data or system.3 In this case, the cybersecurity criminal was able to access an encrypted file system and overwrite parts of some files with random data. This means that the data in those files was altered without authorization and became unusable or invalid. This is a clear example of an integrity breach, as it violated the principle of ensuring that data is accurate and consistent throughout its lifecycle.4 Reference := CCAK Study Guide, Chapter 4: A Threat Analysis Methodology for Cloud Using CCM, page 811; What is CIA Triad? Definition and Examples2; Data Integrity vs Data Security: What's The Difference?3; Data Integrity: Definition & Examples

Question: 19

Which of the following is the GREATEST risk associated with hidden interdependencies between cloud services?

A. The IT department does not clearly articulate the cloud to the organization.
B. There is a lack of visibility over the cloud service providers' supply chain.
C. Customers do not understand cloud technologies in enough detail.
D. Cloud services are very complicated.

Answer: B

Explanation:
The greatest risk associated with hidden interdependencies between cloud services is the lack of visibility over the cloud service providers' supply chain. Hidden interdependencies are the complex and often unknown relationships and dependencies between different cloud services, providers, subproviders, and customers. These interdependencies can create challenges and risks for the security, availability, performance, and compliance of the cloud services and data. For example, a failure or breach in one cloud service can affect other cloud services that depend on it, or a change in one cloud provider's policy or contract can impact other cloud providers or customers that rely on it.12 The lack of visibility over the cloud service providers' supply chain means that the customers do not have enough information or control over how their cloud services and data are delivered, managed, and protected by the providers and their sub-providers. This can expose the customers to various threats and vulnerabilities, such as data breaches, data loss, service outages, compliance violations, legal disputes, or contractual conflicts. The customers may also face difficulties in monitoring, auditing, or verifying the security and compliance status of their cloud services and data across the supply chain. Therefore, it is important for the customers to understand the hidden interdependencies between cloud services and to establish clear and transparent agreements with their cloud providers and sub-providers regarding their roles, responsibilities, expectations, and obligations.3
Reference := How to identify and map service dependencies - Gremlin1; Mitigate Risk for Data Center Network Migration - Cisco2; Practical Guide to Cloud Service Agreements Version 2.03; HIDDEN INTERDEPENDENCIES BETWEEN INFORMATION AND ORGANIZATIONAL …

Question: 20

It is MOST important for an auditor to be aware that an inventory of assets within a cloud environment:

A. should be mapped only if discovered during the audit.
B. is not fundamental for the security management program, as this is a cloud service.
C. can be a misleading source of data.
D. is fundamental for the security management program

Answer: D

Explanation:
It is most important for an auditor to be aware that an inventory of assets within a cloud environment is fundamental for the security management program. An inventory of assets is a list of all the hardware, software, data, and services that are owned, used, or managed by an organization in the cloud. An inventory of assets helps the organization to identify, classify, and prioritize its cloud resources and to implement appropriate security controls and policies to protect them. An inventory of assets also helps the organization to comply with relevant regulations, standards, and contracts that may apply to its cloud environment.12
An auditor should be aware of the importance of an inventory of assets in the cloud because it provides a baseline for assessing the security posture and compliance status of the organization's cloud

environment. An auditor can use the inventory of assets to verify that the organization has a clear and accurate understanding of its cloud resources and their characteristics, such as location, ownership, configuration, dependencies, vulnerabilities, and risks. An auditor can also use the inventory of assets to evaluate whether the organization has implemented adequate security measures and processes to protect its cloud resources from threats and incidents. An auditor can also use the inventory of assets to identify any gaps or weaknesses in the organization's security

management program and to provide recommendations for improvement.34
Reference := Why is IT Asset Inventory Management Critical? - Fresh Security1; Use asset inventory to manage your resources' security posture2; The importance of asset inventory in cybersecurity3; The Importance Of Asset Inventory In Cyber Security And CMDB - Visore4

Question: 21

What do cloud service providers offer to encourage clients to extend the cloud platform?

A. Cloud console
B. Reward programs
C. Access to the cloud infrastructure
D. Application programming interfaces (APIs)

Answer: D

Explanation:
Cloud service providers offer application programming interfaces (APIs) to encourage clients to extend the cloud platform. APIs are sets of rules and protocols that define how different software components or applications can communicate and interact with each other. APIs enable clients to access the cloud services and data, integrate them with their own applications or systems, and customize or enhance their functionality and performance. APIs also allow clients to leverage the cloud platform's features and capabilities, such as scalability, reliability, security, and analytics.12 Some examples of cloud service providers that offer APIs are Google Cloud, Microsoft Azure, Amazon Web Services (AWS), IBM Cloud, and Oracle Cloud. These providers offer various types of APIs for different purposes and domains, such as compute, storage, database, networking, artificial intelligence, machine learning, big data, internet of things, and blockchain. These APIs help clients to build, deploy, manage, and optimize their cloud applications and solutions.34567
Reference := What is an API? - Definition from WhatIs.com1; What is a Cloud API? - Definition from Techopedia2; Cloud APIs | Google Cloud3; Cloud Services - Deploy Cloud Apps & APIs | Microsoft Azure4; AWS Application Programming Interface (API) | AWS5; IBM Cloud API Docs6; Oracle Cloud Infrastructure API Documentation

Question: 22

Regarding suppliers of a cloud service provider, it is MOST important for the auditor to be aware that the:

A. client organization has a clear understanding of the provider s suppliers.
B. suppliers are accountable for the provider's service that they are providing.
C. client organization does not need to worry about the provider's suppliers, as this is the provider's responsibility.
D. client organization and provider are both responsible for the provider's suppliers.

Answer: A

Explanation:

Regarding suppliers of a cloud service provider, it is most important for the auditor to be aware that the client organization has a clear understanding of the provider's suppliers. This is because cloud services often involve multiple parties in the supply chain, such as cloud providers, sub-providers, brokers, carriers, and auditors. Each party may have different roles and responsibilities in delivering the cloud services and ensuring their quality, security, and compliance. Therefore, it is essential for the client organization to have visibility and assurance of the performance and compliance of the provider's suppliers and to establish clear and transparent agreements with them regarding their roles, responsibilities, expectations, and obligations.12

An auditor should be aware of the importance of the client organization's understanding of the provider's suppliers because it provides a basis for assessing the risks and challenges associated with outsourcing services to a cloud provider and its supply chain. An auditor can use the client organization's understanding of the provider's suppliers to verify that the client organization has conducted a thorough due diligence of the provider's suppliers and their capabilities, qualifications, certifications, and reputation. An auditor can also use the client organization's understanding of the provider's suppliers to evaluate whether the client organization has implemented adequate controls and processes to monitor, audit, or verify the security and compliance status of their cloud services and data across the supply chain. An auditor can also use the client organization's understanding of the provider's suppliers to identify any gaps or weaknesses in the client organization's security management program and to provide recommendations for improvement.34 Reference := Practical Guide to Cloud Service Agreements Version 2.01; HIDDEN INTERDEPENDENCIES BETWEEN INFORMATION AND ORGANIZATIONAL …2; Cloud Computing: The Audit Challenge - ISACA3; Cloud Computing: Audit Considerations - AICPA4

Question: 23

Which of the following MOST enhances the internal stakeholder decision-making process for the remediation of risks identified from an organization's cloud compliance program?

A. Establishing ownership and accountability
B. Reporting emerging threats to senior stakeholders
C. Monitoring key risk indicators (KRIs) for multi-cloud environments
D. Automating risk monitoring and reporting processes

Answer: A

Explanation:

The most effective way to enhance the internal stakeholder decision-making process for the remediation of risks identified from an organization's cloud compliance program is to establish ownership and accountability for each risk and its corresponding control. Ownership and accountability mean that the stakeholders who are responsible for managing, implementing, monitoring, and reporting on the cloud compliance program have clearly defined roles, responsibilities, expectations, and authorities. Ownership and accountability also mean that the stakeholders who are affected by or involved in the cloud compliance program have sufficient awareness, communication, collaboration, and feedback mechanisms. Establishing ownership and accountability helps to ensure that the risks and controls are properly identified, assessed, prioritized, treated, and reviewed in a timely and consistent manner. It also helps to foster a culture of trust, transparency, and accountability among the internal stakeholders and to align their goals and interests with the organization's

cloud compliance objectives.1 [2][2]

Reference := CCAK Study Guide, Chapter 3: Cloud Compliance Program, page 521; Cloud Compliance: A Framework for Using Cloud Services While Maintaining Data Protection Compliance[

Question: 24

Visibility to which of the following would give an auditor the BEST view of design and implementation decisions when an organization uses programmatic automation for Infrastructure as a Service (IaaS) deployments?

A. Source code within build scripts
B. Output from threat modeling exercises
C. Service level agreements (SLAs)
D. Results from automated testing

Answer: A

Explanation:
Visibility to the source code within build scripts would give an auditor the best view of design and implementation decisions when an organization uses programmatic automation for Infrastructure as a Service (IaaS) deployments. IaaS is a cloud service model that provides virtualized computing resources, such as servers, storage, network, and operating systems, over the internet. Programmatic automation is the process of using code or scripts to automate the provisioning, configuration, management, and monitoring of the cloud infrastructure. Build scripts are files that contain commands or instructions to create or modify the cloud infrastructure according to the desired specifications.12
An auditor can use the source code within build scripts to gain insight into how the organization designs and implements its cloud infrastructure. The source code can reveal the following information3:
The type, size, and number of cloud resources that are provisioned and deployed The configuration settings and parameters that are applied to the cloud resources The security controls and policies that are enforced on the cloud resources The dependencies and relationships between the cloud resources
The testing and validation methods that are used to verify the functionality and performance of the cloud resources
The logging and auditing mechanisms that are used to track and record the changes and activities on the cloud resources
By reviewing the source code within build scripts, an auditor can evaluate whether the organization follows the best practices and standards for cloud infrastructure design and implementation, such as scalability, reliability, security, compliance, and efficiency. An auditor can also identify any gaps or risks in the organization's cloud infrastructure and provide recommendations for improvement. Reference := What is Infrastructure as Code? | Cloud Computing - AWS1; What is Programmatic Automation? - Definition from Techopedia2; How to audit your IaC for better DevSecOps - TechBeacon3

Question: 25

The MAIN limitation of relying on traditional cloud compliance assurance approaches such as SOC2 attestations is that:

A. they can only be performed by skilled cloud audit service providers.
B. they are subject to change when the regulatory climate changes.
C. they provide a point-in-time snapshot of an organization's compliance posture.
D. they place responsibility for demonstrating compliance on the vendor organization.

Answer: C

Explanation:
Traditional cloud compliance assurance approaches such as SOC2 attestations have the main limitation of providing a point-in-time snapshot of an organization's compliance posture. This means that they only reflect the state of the organization's security and compliance controls at a specific date or period, which may not be representative of the current or future state. Cloud environments are dynamic and constantly changing, and so are the threats and risks that affect them. Therefore, relying on traditional cloud compliance assurance approaches may not provide sufficient or timely assurance that the organization's cloud services and data are adequately protected and compliant with the relevant requirements and standards.12
To overcome this limitation, some organizations adopt continuous cloud compliance assurance approaches, such as continuous monitoring, auditing, and reporting. These approaches enable the organization to collect, analyze, and report on the security and compliance status of its cloud environment in near real-time, using automated tools and processes. Continuous cloud compliance assurance approaches can help the organization to identify and respond to any changes, issues, or incidents that may affect its cloud security and compliance posture, and to maintain a high level of trust and transparency with its stakeholders, customers, and regulators.34
Reference := What is SOC 2? Complete Guide to SOC 2 Reports | CSA1; Guidance on cloud security assessment and authorization - ITSP.50.105 - Canadian Centre for Cyber Security2; Continuous Compliance: The Future of Cloud Security | CloudCheckr3; Continuous Compliance: How to Automate Cloud Security Compliance4

Question: 26

An organization that is utilizing a community cloud is contracting an auditor to conduct a review on behalf of the group of organizations within the cloud community. Of the following, to whom should the auditor report the findings?

A. Management of the organization being audited
B. Shareholders and interested parties
C. Cloud service provider
D. Public

Answer: A

Explanation:
According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the auditor should report the findings to the management of the organization being audited, as they are the primary stakeholders and decision makers for the audit. The management is responsible for ensuring that the cloud service provider meets the contractual obligations and service level agreements, as well as the security and compliance requirements of the community cloud. The auditor should also communicate with the cloud service provider and other relevant parties, such as regulators or customers, as appropriate, but the final report should be addressed to the management of the organization being audited. Reference: ISACA Cloud Auditing Knowledge Certificate Study Guide, page 17

Question: 27

Which of the following standards is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an information security management system based on ISO/IEC 27001?

A. ISO/IEC 27017:2015
B. ISO/IEC 27002
C. NIST SP 800-146
D. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Answer: A

Explanation:

ISO/IEC 27017:2015 is a standard that provides guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002, as well as additional controls with implementation guidance that specifically relate to cloud services1. ISO/IEC 27017:2015 is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an information security management system based on ISO/IEC 270011. ISO/IEC 27001 is a standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

ISO/IEC 27002 is a standard that provides a code of practice for information security controls, but it does not provide specific guidance for cloud services. NIST SP 800-146 is a publication that provides an overview of cloud computing, its characteristics, service models, deployment models, and security considerations, but it does not provide a standard for selecting controls for cloud services. CSA CCM is a framework that provides detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains, but it is not a standard that is based on ISO/IEC 27001. Reference: ISO/IEC 27017:2015 [ISO/IEC 27001:2013] [ISO/IEC 27002:2013] [NIST SP 800-146] [CSA CCM]

Question: 28

During an audit, it was identified that a critical application hosted in an off-premises cloud is not part of the organization's disaster recovery plan (DRP). Management stated that it is responsible for

ensuring the cloud service provider has a plan that is tested annually. What should be the auditor's NEXT course of action?

A. Review the security white paper of the provider.
B. Review the provider's audit reports.
C. Review the contract and DR capability.
D. Plan an audit of the provider

Answer: C

Explanation:

The auditor's next course of action should be to review the contract and DR capability of the cloud service provider. This will help the auditor to verify if the provider has a DR plan that meets the

organization's requirements and expectations, and if the provider has evidence of testing and validating the plan annually. The auditor should also check if the contract specifies the roles and responsibilities of both parties, the RTO and RPO values, the SLA terms, and the penalties for noncompliance. Reviewing the security white paper of the provider (option A) might give some information about the provider's security practices and controls, but it might not be sufficient or relevant to assess the DR plan. Reviewing the provider's audit reports (option B) might also provide some assurance about the provider's compliance with standards and regulations, but it might not address the specific DR needs of the organization. Planning an audit of the provider (option D) might be a possible course of action, but it would require more time and resources, and it might not be feasible or necessary if the contract and DR capability are already satisfactory. Reference:
Disaster recovery planning guide
Audit a Disaster Recovery Plan
How to Maintain and Test a Business Continuity and Disaster Recovery Plan

Question: 29

Which of the following is the BEST tool to perform cloud security control audits?

A. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
B. General Data Protection Regulation (GDPR)
C. Federal Information Processing Standard (FIPS) 140-2
D. ISO 27001

Answer: A

Explanation:
The CSA Cloud Controls Matrix (CCM) is the best tool to perform cloud security control audits, as it is a cybersecurity control framework for cloud computing that is aligned to the CSA best practices and is considered the de-facto standard for cloud security and privacy1. The CCM provides a set of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology, such as identity and access management, data security, encryption and key management, business continuity and disaster recovery, audit assurance and compliance, and risk management1. The CCM also maps the controls to various industry-accepted security standards, regulations, and control

frameworks, such as ISO 27001/27002/27017/27018, NIST SP 800-53, PCI DSS, GDPR, and others1. The CCM can be used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain1. The CCM also includes the Consensus Assessment Initiative Questionnaire (CAIQ), which provides a set of "yes or no" questions based on the security controls in the CCM that can be used to assess a cloud service provider2.
The other options are not the best tools to perform cloud security control audits, as they are either not specific to cloud computing or not comprehensive enough. GDPR is a regulation that aims to protect the personal data and privacy of individuals in the European Union and the European Economic Area3, but it does not provide a framework for cloud security controls. FIPS 140-2 is a standard that specifies the security requirements for cryptographic modules used by federal agencies in the United States, but it does not cover other aspects of cloud security. ISO 27001 is a standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization, but it does not provide specific guidance for cloud services. Reference: Cloud Controls Matrix (CCM) - CSA

Cloud Controls Matrix and CAIQ v4 | CSA - Cloud Security Alliance

General Data Protection Regulation - Wikipedia [FIPS 140-2 - Wikipedia] [ISO/IEC 27001:2013]

Question: 30

When an organization is using cloud services, the security responsibilities largely vary depending on the service delivery model used, while the accountability for compliance should remain with the:

A. cloud user.
B. cloud service provider. 0
C. cloud customer.
D. certification authority (CA)

Answer: C

Explanation:

According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the cloud customer is the entity that retains accountability for the business outcome of the system or the processes that are supported by the cloud service1. The cloud customer is also responsible for ensuring that the cloud service meets the legal, regulatory, and contractual obligations that apply to the customer's business context1. The cloud customer should also perform due diligence and risk assessment before selecting a cloud service provider, and establish a clear and enforceable contract that defines the roles and responsibilities of both parties1.

The cloud user is the entity that uses the cloud service on behalf of the cloud customer, but it is not necessarily accountable for the compliance of the service1. The cloud service provider is the entity that makes the cloud service available to the cloud customer, but it is not accountable for the compliance of the customer's business context1. The certification authority (CA) is an entity that issues digital certificates to verify the identity or authenticity of other entities, but it is not accountable for the compliance of the cloud service2.

Reference:

ISACA Cloud Auditing Knowledge Certificate Study Guide, page 10-11.

Certification authority - Wikipedia

Question: 31

A cloud service provider utilizes services of other service providers for its cloud service. Which of the following is the BEST approach for the auditor while performing the audit for the cloud service?

A. The auditor should review the service providers' security controls even more strictly, as they are further separated from the cloud customer.
B. The auditor should review the relationship between the cloud service provider and its service provider to help direct and estimate the level of effort and analysis the auditor should apply.
C. As the contract for the cloud service is between the cloud customer and the cloud service provider, there is no need for the auditor to review the services provided by the service providers.
D. As the relationship between the cloud service provider and its service providers is governed by separate contracts between them, there is no need for the auditor to review the services

Answer: B

Explanation:

According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the auditor should review the relationship between the cloud service provider and its service provider to help direct and estimate the level of effort and analysis the auditor should apply1. The auditor should understand the nature and scope of the services provided by the service provider, the contractual obligations and service level agreements, the security and compliance requirements, and the monitoring and reporting mechanisms. The auditor should also assess the risks and controls associated with the service provider, and determine if additional audit procedures are needed to obtain sufficient assurance.

The other options are not the best approach for the auditor. Option A is too strict and might not be feasible or necessary, depending on the type and level of services provided by the service provider. Option C is too lax and might overlook significant risks and gaps in the cloud service. Option D is too narrow and might ignore the impact of the service provider on the cloud customer's business context. Reference:

ISACA Cloud Auditing Knowledge Certificate Study Guide, page 13-14.

Question: 32

The PRIMARY objective for an auditor to understand the organization's context for a cloud audit is to:

A. determine whether the organization has carried out control self-assessment (CSA) and validated audit reports of the cloud service providers.

B. validate an understanding of the organization's current state and how the cloud audit plan fits into the existing audit approach.

C. validate the organization's performance effectiveness utilizing cloud service provider solutions.

D. validate whether an organization has a cloud audit plan in place.

Answer: B

Explanation:

According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the primary objective for an auditor to understand the organization's context for a cloud audit is to validate an understanding of the organization's current state and how the cloud audit plan fits into the existing audit approach1. The auditor should consider the organization's business objectives, strategies, risks, and opportunities, as well as the regulatory and contractual requirements that apply to the organization's use of cloud services. The auditor should also assess the organization's cloud maturity level, governance structure, policies and procedures, roles and responsibilities, and existing controls related to cloud services. The auditor should then align the cloud audit plan with the organization's context and ensure that it covers the relevant scope, objectives, criteria, and methodology.

The other options are not the primary objective for an auditor to understand the organization's context for a cloud audit. Option A is a possible audit procedure, but not the main goal of understanding the organization's context. Option C is a possible audit outcome, but not the main purpose of understanding the organization's context. Option D is a possible audit finding, but not the main reason for understanding the organization's context. Reference: ISACA Cloud Auditing Knowledge Certificate Study Guide, page 12-13.

Question: 33

During the planning phase of a cloud audit, the PRIMARY goal of a cloud auditor is to:

A. specify appropriate tests.
B. address audit objectives.
C. minimize audit resources.
D. collect sufficient evidence.

Answer: B

Explanation:
According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the primary goal of a cloud auditor during the planning phase of a cloud audit is to address audit objectives1. The audit objectives are the specific questions that the audit aims to answer, such as whether the cloud service meets the security, compliance, performance, and availability requirements of the cloud customer. The audit objectives should be aligned with the organization's context, risk appetite, and expectations. The audit objectives should also be clear, measurable, achievable, relevant, and timely. The other options are not the primary goal of a cloud auditor during the planning phase of a cloud audit. Option A is a possible activity, but not the main goal of the planning phase. The appropriate tests are determined based on the audit objectives, criteria, and methodology. Option C is a possible constraint, but not the main goal of the planning phase. The audit resources should be allocated based on the audit scope, complexity, and significance. Option D is a possible outcome, but not the main goal of the planning phase. The sufficient evidence is collected during the execution phase of the audit, based on the audit plan. Reference:
ISACA Cloud Auditing Knowledge Certificate Study Guide, page 12-13.

Question: 34

An auditor examining a cloud service provider's service level agreement (SLA) should be MOST

concerned about whether:

A. the agreement includes any operational matters that are material to the service operations.
B. the agreement excludes any sourcing and financial matters that are material in meeting the service level agreement (SLA).
C. the agreement includes any service availability matters that are material to the service operations.
D. the agreement excludes any operational matters that are material to the service operations

Answer: D

Explanation:
An auditor examining a cloud service provider's SLA should be most concerned about whether the agreement excludes any operational matters that are material to the service operations, as this could indicate a lack of transparency, accountability, and quality assurance from the provider. Operational matters are the aspects of the cloud service that affect its functionality, performance, availability, reliability, security, and compliance. Examples of operational matters include service scope, roles and responsibilities, service levels and metrics, monitoring and reporting mechanisms, incident and problem management, change management, backup and recovery, data protection and privacy, and termination and exit clauses12. These matters are material to the

service operations if they have a significant impact on the achievement of the service objectives and expectations of the cloud customer. The auditor should verify that the SLA covers all the relevant and material operational matters in a clear and comprehensive manner, and that the provider adheres to the SLA terms and conditions.

The other options are not the most concerning for the auditor. Option A is a desirable feature of an SLA, but not a concern if it is missing. Option B is an unrealistic expectation of an SLA, as sourcing and financial matters are usually essential in meeting the SLA. Option C is a specific example of an operational matter that is material to the service operations, but not the only one that should be included in the SLA. Reference:

Cloud Services Due Diligence Checklist

Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance

Question: 35

A cloud auditor should use statistical sampling rather than judgment (nonstatistical) sampling when:

A. generalized audit software is unavailable.
B. the auditor wants to avoid sampling risk.
C. the probability of error must be objectively quantified.
D. the tolerable error rate cannot be determined.

Answer: C

Explanation:

According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, a cloud auditor should use statistical sampling rather than judgment (nonstatistical) sampling when the probability of error must be objectively quantified1. Statistical sampling is a sampling technique that uses random selection methods and mathematical calculations to draw conclusions about the population from the sample results. Statistical sampling allows the auditor to measure the sampling risk, which is the risk that the sample results do not represent the population, and to express the confidence level and precision of the sample1. Statistical sampling also enables the auditor to estimate the rate of exceptions or errors in the population based on the sample1.

The other options are not valid reasons for using statistical sampling rather than judgment sampling. Option A is irrelevant, as generalized audit software is a tool that can facilitate both statistical and judgment sampling, but it is not a requirement for either technique. Option B is incorrect, as statistical sampling does not avoid sampling risk, but rather measures and controls it. Option D is illogical, as the tolerable error rate is a parameter that must be determined before conducting any sampling technique, whether statistical or judgmental. Reference: ISACA Cloud Auditing Knowledge Certificate Study Guide, page 17-18.

Question: 36

The FINAL decision to include a material finding in a cloud audit report should be made by the:

A. auditee's senior management.
B. organization's chief executive officer (CEO).
C. cloud auditor.
: D. organization's chief information security officer (CISO)

Answer: C

Explanation:

According to the ISACA Cloud Auditing Knowledge Certificate Study Guide, the final decision to include a material finding in a cloud audit report should be made by the cloud auditor1. A material finding is a significant error or risk in the cloud service that could affect the achievement of the audit objectives or the cloud customer's business outcomes. The cloud auditor is responsible for identifying, evaluating, and reporting the material findings based on the audit criteria, methodology, and evidence. The cloud auditor should also communicate the material findings to the auditee and other relevant stakeholders, and obtain their feedback and responses.

The other options are not correct. Option A is incorrect, as the auditee's senior management is not in charge of the audit report, but rather the subject of the audit. The auditee's senior management should provide their perspective and action plans for the material findings, but they cannot decide whether to include or exclude them from the report. Option B is incorrect, as the organization's CEO is not involved in the audit process, but rather the ultimate recipient of the audit report. The organization's CEO should review and act upon the audit report, but they cannot influence the content of the report. Option D is incorrect, as the organization's CISO is not an independent party, but rather a stakeholder of the audit. The organization's CISO should support and collaborate with the cloud auditor, but they cannot make the final decision on the material findings. Reference: ISACA Cloud Auditing Knowledge Certificate Study Guide, page 19-20.

Question: 37

What aspect of Software as a Service (SaaS) functionality and operations would the cloud customer be responsible for and should be audited?

A. Access controls
B. Vulnerability management
C. Patching
D. Source code reviews

Answer: A

Explanation:

According to the cloud shared responsibility model, the cloud customer is responsible for managing the access controls for the SaaS functionality and operations, and this should be audited by the cloud auditor12. Access controls are the mechanisms that restrict and regulate who can access and use the SaaS applications and data, and how they can do so. Access controls include identity and access management, authentication, authorization, encryption, logging, and monitoring. The cloud customer is responsible for defining and enforcing the access policies, roles, and permissions for the SaaS users, as well as ensuring that the access controls are aligned with the security and compliance requirements of the customer's business context12.

The other options are not the aspects of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Option B is incorrect, as vulnerability management is the process of identifying, assessing, and mitigating the security weaknesses in the SaaS applications and infrastructure, and this is usually handled by the cloud service provider12. Option C is incorrect, as patching is the process of updating and fixing the SaaS applications and infrastructure to address security issues or improve performance, and this is also usually handled by the cloud service provider12. Option D is incorrect, as source code reviews are the process of examining and testing the SaaS applications' source code to detect errors or vulnerabilities,

and this is also usually handled by the cloud service provider12. Reference:
Shared responsibility in the cloud - Microsoft Azure
The Customer's Responsibility in the Cloud Shared Responsibility Model - ISACA

Question: 38

What areas should be reviewed when auditing a public cloud?

A. Identity and access management (IAM) and data protection
B. Source code reviews and hypervisor
C. Patching and configuration
D. Vulnerability management and cyber security reviews

Answer: A

Explanation:
When auditing a public cloud, it is essential to review areas such as Identity and Access Management (IAM) and data protection. IAM involves ensuring that only authorized individuals have access to the cloud resources, and that their access is appropriately managed and monitored. This includes reviewing user authentication methods, access control policies, role-based access controls, and user activity monitoring1.
Data protection is another critical area to review. It involves ensuring that the data stored in the public cloud is secure from unauthorized access, breaches, and leaks. This includes reviewing data encryption methods, data backup and recovery processes, data privacy policies, and compliance with relevant data protection regulations1.
While the other options may also be relevant in certain contexts, they are not as universally applicable as IAM and data protection for auditing a public cloud. Source code reviews and hypervisor (option B), patching and configuration (option C), and vulnerability management and cybersecurity reviews (option D) are important but are more specific to certain types of cloud services or deployment models. Reference:
Cloud Computing — What IT Auditors Should Really Know - ISACA

Question: 39

Which of the following aspects of risk management involves identifying the potential reputational and financial harm when an incident occurs?

A. Impact analysis
B. Likelihood
C. Mitigation
D. Residual risk

Answer: A

Explanation:
According to the web search results, impact analysis is the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Impact analysis is the process of assessing the probabilities and consequences of risk events if they are realized1. Impact analysis helps to understand how project outcomes and objectives might change due to the impact of the risk event, and to measure the severity of the risk impact in terms of cost, schedule, quality, and other factors23. Impact analysis

also helps to prioritize the risks and plan appropriate responses and controls23.

The other options are not correct. Likelihood is the aspect of risk management that involves estimating the probability or frequency of a risk event occurring23. Mitigation is the aspect of risk management that involves implementing actions or controls to reduce the likelihood or impact of a risk event23. Residual risk is the aspect of risk management that involves measuring the remaining risk after applying mitigation actions or controls23. Reference:

Risk Analysis: Definition, Examples and Methods - ProjectManager

Risk Assessment and Analysis Methods: Qualitative and Quantitative - ISACA Systems Engineering: Risk Impact Assessment and Prioritization

Question: 40

Which of the following would be the MOST critical finding of an application security and DevOps audit?

A. Certifications with global security standards specific to cloud are not reviewed, and the impact of noted findings are not assessed.

B. Application architecture and configurations did not consider security measures.

C. Outsourced cloud service interruption, breach, or loss of stored data occurred at the cloud service provider.

D. The organization is not using a unified framework to integrate cloud compliance with regulatory requirements

Answer: B

Explanation:

According to the web search results, the most critical finding of an application security and DevOps audit would be that the application architecture and configurations did not consider security measures. This finding indicates a serious lack of security by design and security by default principles, which are essential for ensuring the confidentiality, integrity, and availability of the application and its data . If the application architecture and configurations are not secure, they could expose the application to various threats and vulnerabilities, such as unauthorized access, data breaches, denial-of-service attacks, injection attacks, cross-site scripting attacks, and others . This finding could also result in non-compliance with relevant security standards and regulations, such as ISO 27001, PCI DSS, GDPR, and others . Therefore, this finding should be addressed with high priority and urgency by implementing appropriate security measures and controls in the application architecture and configurations.

The other options are not as critical as option B. Option A is a moderate finding that indicates a lack of awareness and assessment of the global security standards specific to cloud, such as ISO 27017, ISO 27018, CSA CCM, NIST SP 800-53, and others . This finding could affect the security and compliance of the cloud services used by the application, but it does not directly impact the application itself. Option C is a severe finding that indicates a major incident that occurred at the cloud service provider level, such as a service interruption, breach, or loss of stored data. This finding could affect the availability, confidentiality, and integrity of the application and its data, but it is not caused by the application itself. Option D is a minor finding that indicates a lack of efficiency and consistency in integrating cloud compliance with regulatory requirements. This finding could affect the compliance posture of the application and its data, but it does not directly impact the security or functionality of the application. Reference: [Application Security Best Practices - OWASP] [DevSecOps: What It Is and How to Get Started - ISACA] [Cloud Security Standards: What to Expect & What to Negotiate - CSA] [Cloud Computing Security Audit -

ISACA]
[Cloud Computing Incident Response - ISACA]
[Cloud Compliance: A Framework for Using Cloud Services While Maintaining Compliance - ISACA]

Question: 41

What legal documents should be provided to the auditors in relation to risk management?

A. Enterprise cloud strategy and policy
B. Contracts and service level agreements (SLAs) of cloud service providers
C. Policies and procedures established around third-party risk assessments
D. Inventory of third-party attestation reports

Answer: B

Explanation:
Contracts and SLAs are legal documents that define the roles, responsibilities, expectations, and obligations of both the cloud service provider (CSP) and the cloud customer. They also specify the terms and conditions for service delivery, performance, availability, security, compliance, data protection, incident response, dispute resolution, liability, and termination. An auditor should review these documents to assess the alignment of the CSP's services with the customer's business requirements and risk appetite, as well as to identify any gaps or inconsistencies that may pose legal risks. Reference:
ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 35-36
Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) v4.0, 2021, GRM-01: Contracts and SLAs

Question: 42

In relation to testing business continuity management and operational resilience, an auditor should review which of the following database documentation?

A. Database backup and replication guidelines
B. System backup documentation
C. Incident management documentation
D. Operational manuals

Answer: A

Explanation:
Database backup and replication guidelines are essential for ensuring the availability and integrity of data in the event of a disruption or disaster. They describe how the data is backed up, stored, restored, and synchronized across different locations and platforms. An auditor should review these guidelines to verify that they are aligned with the business continuity objectives, policies, and procedures of the organization and the cloud service provider. The auditor should also check that the backup and replication processes are tested regularly and that the results are documented and reported. Reference:
ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 96
Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) v4.0, 2021, BCR-01: Business Continuity Planning/Resilience

Question: 43

The MOST critical concept for managing the building and testing of code in DevOps is:

A. continuous build.
B. continuous delivery.
C. continuous integration.
D. continuous deployment.

Answer: C

Explanation:

Continuous integration (CI) is the most critical concept for managing the building and testing of code in DevOps. CI is the practice of merging all developers' working copies of code to a shared mainline several times a day. This enables early detection and resolution of bugs, conflicts, and errors, as well as faster and more frequent feedback loops. CI also facilitates the automation of building, testing, and deploying code, which improves the quality, reliability, and security of the software delivery process. CI is a prerequisite for continuous delivery (CD) and continuous deployment (CD), which are the next stages of DevOps maturity that aim to deliver software to customers faster and more frequently. Reference:

ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 114-115

Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM) v4.0, 2021, DCS-01: Datacenter Security - Build and Test

What is Continuous Integration?

Continuous Integration vs Continuous Delivery vs Continuous Deployment

Question: 44

What is a sign that an organization has adopted a shift-left concept of code release cycles?

A. Large entities with slower release cadences and geographically dispersed systems
B. A waterfall model to move resources through the development to release phases
C. Maturity of start-up entities with high-iteration to low-volume code commits
D. Incorporation of automation to identify and address software code problems early

Answer: D

Explanation:

The shift-left concept of code release cycles is an approach that moves testing, quality, and performance evaluation early in the development process, often before any code is written. The goal of shift-left testing is to anticipate and resolve software defects, bugs, errors, and vulnerabilities as soon as possible, reducing the cost and time of fixing them later in the production stage. To achieve this, shift-left testing relies on automation tools and techniques that enable continuous integration, continuous delivery, and continuous deployment of code. Automation also facilitates collaboration and feedback among developers, testers, security experts, and other stakeholders throughout the development lifecycle. Therefore, the incorporation of automation to identify and address software code problems early is a sign that an organization has adopted a shift-left concept of code release cycles. Reference:

The 'Shift Left' Is A Growing Theme For Cloud Cybersecurity In 2022

Shift left vs shift right: A DevOps mystery solved

How to shift left with continuous integration

Question: 45

Which of the following can be used to determine whether access keys are stored in the source code or any other configuration files during development?

A. Static code review
B. Dynamic code review
C. Vulnerability scanning
D. Credential scanning

Answer: D

Explanation:
Credential scanning is a technique that can be used to detect and prevent the exposure of access keys and other sensitive information in the source code or any other configuration files during development. Credential scanning tools can scan the code repositories, files, and commits for any hardcoded credentials, such as access keys, passwords, tokens, certificates, and connection strings. They can also alert the developers or security teams of any potential leaks and suggest remediation actions, such as rotating or revoking the compromised keys, removing the credentials from the code, or using secure storage mechanisms like vaults or environment variables. Credential scanning can be integrated into the development pipeline as part of the continuous integration and continuous delivery (CI/CD) process, or performed periodically as a security audit. Credential scanning can help reduce the risk of credential leakage, which can lead to unauthorized access, data breaches, or account compromise. Reference:

Protecting Source Code in the Cloud with DSPM Best practices for managing service account keys Protect your code repository

Question: 46

What is an advantage of using dynamic application security testing (DAST) over static application security testing (SAST) methodology?

A. DAST is slower but thorough.
B. Unlike SAST, DAST is a black box and programming language agnostic.
C. DAST can dynamically integrate with most continuous integration and continuous delivery (CI/CD) tools.
D. DAST delivers more false positives than SAST

Answer: B

Explanation:
Dynamic application security testing (DAST) is a method of testing the security of an application by simulating attacks from an external source. DAST does not require access to the source code or binaries of the application, unlike static application security testing (SAST), which analyzes the code for vulnerabilities. Therefore, DAST is a black box testing technique, meaning that it does not need any knowledge of the internal structure, design, or implementation of the application. DAST is also programming language agnostic, meaning that it can test applications written in any language, framework, or platform. This makes DAST more flexible and adaptable to different types of applications and environments. However, DAST also has some limitations, such as being

slower, less accurate, and more dependent on the availability and configuration of the application. Reference:

SAST vs. DAST: What's the Difference?

SAST vs DAST: What's the Difference?

SAST vs. DAST: Enhancing application security

Question: 47

Which of the following BEST ensures adequate restriction on the number of people who can access the pipeline production environment?

A. Separation of production and development pipelines
B. Ensuring segregation of duties in the production and development pipelines
C. Role-based access controls in the production and development pipelines
D. Periodic review of the continuous integration and continuous delivery (CI/CD) pipeline audit logs to identify any access violations

Answer: C

Explanation:

Role-based access controls (RBAC) are a method of restricting access to resources based on the roles of individual users within an organization. RBAC allows administrators to assign permissions to roles, rather than to specific users, and then assign users to those roles. This simplifies the management of access rights and reduces the risk of unauthorized or excessive access. RBAC is especially important for ensuring adequate restriction on the number of people who can access the pipeline production environment, which is the final stage of the continuous integration and continuous delivery (CI/CD) process where code is deployed to the end-users. Access to the production environment should be limited to only those who are responsible for deploying, monitoring, and maintaining the code, such as production engineers, release managers, or site reliability engineers. Developers, testers, or other stakeholders should not have access to the production environment, as this could compromise the security, quality, and performance of the code. RBAC can help enforce this separation of duties and responsibilities by defining different roles for different pipeline stages and granting appropriate permissions to each role. For example, developers may have permission to create, edit, and test code in the development pipeline, but not to deploy or modify code in the production pipeline. Conversely, production engineers may have permission to deploy, monitor, and troubleshoot code in the production pipeline, but not to create or edit code in the development pipeline. RBAC can also help implement the principle of least privilege, which states that users should only have the minimum level of access required to perform their tasks. This reduces the attack surface and minimizes the potential damage in case of a breach or misuse. RBAC can be configured at different levels of granularity, such as at the organization, project, or object level, depending on the needs and complexity of the organization. RBAC can also leverage existing identity and access management (IAM) solutions, such as Azure Active Directory or AWS IAM, to integrate with cloud services and applications.

Reference:

Set pipeline permissions - Azure Pipelines

Azure DevOps: Access, Roles and Permissions

Cloud Computing — What IT Auditors Should Really Know

Question: 48

The PRIMARY purpose of Open Certification Framework (OCF) for the CSA STAR program is to:

A. facilitate an effective relationship between the cloud service provider and cloud client. B. enable the cloud service provider to prioritize resources to meet its own requirements. C. provide global, accredited, and trusted certification of the cloud service provider.
D. ensure understanding of true risk and perceived risk by the cloud service users

Answer: C

Explanation:
The primary purpose of the Open Certification Framework (OCF) for the CSA STAR program is to provide global, accredited, and trusted certification of the cloud service provider. According to the CSA website1, the OCF is an industry initiative to allow global, trusted independent evaluation of cloud providers. It is a program for flexible, incremental and multi-layered cloud provider certification and/or attestation according to the Cloud Security Alliance's industry leading security guidance and control framework. The OCF aims to address the gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services. The OCF also integrates with popular third-party assessment and attestation statements developed within the public accounting community to avoid duplication of effort and cost. The OCF manages the foundation that runs and monitors the CSA STAR Certification program, which is an assurance framework that enables cloud service providers to embed cloud-specific security controls. The STAR Certification program has three levels of assurance, each based on a different type of audit or assessment: Level 1: Self-Assessment, Level 2: Third-Party Audit, and Level 3: Continuous Auditing. The OCF also oversees the CSA STAR Registry, which is a publicly accessible repository that documents the security controls provided by various cloud computing offerings2.
The OCF helps consumers to evaluate and compare their providers' resilience, data protection, privacy capabilities, and service portability. It also helps providers to demonstrate their compliance with industry standards and best practices.

Reference:
Open Certification Framework Working Group | CSA
STAR | CSA

Question: 49

An auditor identifies that a cloud service provider received multiple customer inquiries and requests for proposal (RFPs) during the last month. Which of the following
What should be the BEST recommendation to reduce the provider's burden?

A. The provider can answer each customer individually.
B. The provider can direct all customer inquiries to the information in the CSA STAR registry.
C. The provider can schedule a call with each customer.
D. The provider can share all security reports with customers to streamline the process

Answer: B

Explanation:
The CSA STAR registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. The registry is based on the Cloud Controls Matrix (CCM), which is a framework of cloud-specific security best practices, and the GDPR Code of Conduct, which is a set of privacy principles for cloud service providers. The registry allows cloud
customers to assess the security and compliance posture of cloud service providers, as well as to compare different providers based on their level of assurance. The registry also reduces the complexity and cost of filling

out multiple customer questionnaires and requests for proposal (RFPs). Therefore, the best recommendation to reduce the provider's burden is to direct all customer inquiries to the information in the CSA STAR registry, which can demonstrate the provider's transparency, trustworthiness, and adherence to industry standards. The provider can also encourage customers to use the Consensus Assessments Initiative Questionnaire (CAIQ), which is a standardized set of questions based on the CCM, to evaluate the provider's security controls. Alternatively, the provider can pursue higher levels of assurance, such as third-party audits or continuous monitoring, to further validate their security and privacy practices and increase customer confidence.

Reference:

STAR Registry | CSA

STAR | CSA

CSA Security Trust Assurance and Risk (STAR) Registry Reaches Notable ...

Why CSA STAR Is Important for Cloud Service Providers - A-LIGN

Question: 50

Which of the following is the MOST important audit scope document when conducting a review of a cloud service provider?

A. Documentation criteria for the audit evidence
B. Testing procedure to be performed
C. Processes and systems to be audited
D. Updated audit work program

Answer: C

Explanation:

The most important audit scope document when conducting a review of a cloud service provider is the document that defines the processes and systems to be audited. This document should clearly identify the objectives, criteria, and boundaries of the audit, as well as the roles and responsibilities of the audit team and the cloud service provider. The document should also specify the scope of the cloud service provider's services, such as the service model, deployment model, geographic location, data classification, and compliance requirements. The document should also describe the scope of the audit evidence, such as the types, sources, methods, and sampling techniques of data collection and analysis. The document should also state the expected deliverables, timelines, and reporting formats of the audit. The document should be agreed upon by both parties before the audit commences.

The document that defines the processes and systems to be audited is essential for ensuring that the audit is relevant, reliable, consistent, and complete. It helps to establish a common understanding and expectation between the auditor and the auditee, as well as to avoid any misunderstandings or conflicts during or after the audit. It also helps to focus the audit on the key risks and controls related to the cloud service provider's operations and performance. It also helps to ensure that the audit complies with the applicable standards, frameworks, and regulations.

Reference:

Cloud Audits and Compliance: What You Need To Know - Linford & Company LLP How to audit the cloud | ICAEW

Auditing Cloud Computing: A Security and Privacy Guide

Question: 51

The BEST method to report continuous assessment of a cloud provider's services to the Cloud Security Alliance (CSA) is through:

A. Cloud Controls Matrix (CCM) assessment by a third-party auditor on a periodic basis.
B. tools selected by the third-party auditor.
C. SOC 2 Type 2 attestation.
D. a set of dedicated application programming interfaces (APIs).

Answer: D

Explanation:

The best method to report continuous assessment of a cloud provider's services to the Cloud Security Alliance (CSA) is through a set of dedicated application programming interfaces (APIs). According to the CSA website1, the STAR Continuous program is a component of the STAR certification that allows cloud service providers to validate their security posture on an ongoing basis. The STAR Continuous program leverages a set of APIs that can integrate with the cloud provider's existing tools and processes, such as security information and event management (SIEM), governance, risk management, and compliance (GRC), or continuous monitoring systems. The APIs enable the cloud provider to collect, analyze, and report security-related data to the CSA STAR registry in near real-time. The APIs also allow the CSA to verify the data and provide feedback to the cloud provider and the customers. The STAR Continuous program aims to provide more transparency, assurance, and trust in the cloud ecosystem by enabling continuous visibility into the security performance of cloud services.

The other methods listed are not suitable for reporting continuous assessment of a cloud provider's services to the CSA. The Cloud Controls Matrix (CCM) assessment by a third-party auditor on a periodic basis is part of the STAR Certification Level 2 program, which provides a point-in-time validation of the cloud provider's security controls. However, this method does not provide continuous assessment or reporting, as it only occurs once every 12 or 24 months2. The tools selected by the third-party auditor may vary depending on the scope, criteria, and methodology of the audit, and they may not be compatible or consistent with the CSA's standards and frameworks. Moreover, the tools may not be able to report the audit results to the CSA STAR registry automatically or frequently. The SOC 2 Type 2 attestation is an independent audit report that evaluates the cloud provider's security controls based on the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria. However, this report is not specific to cloud computing and does not cover all aspects of the CCM. Furthermore, this report is not intended to be shared publicly or reported to the CSA STAR registry3.

Reference:

STAR Continuous | CSA
STAR Certification | CSA
SOC 2 vs CSA STAR: Which One Should You Choose?

Question: 52

To support a customer's verification of the cloud service provider claims regarding its responsibilities according to the shared responsibility model, which of the following tools and techniques is appropriate?

A. External audit
B. Internal audit
C. Contractual agreement

D. Security assessment

Answer: C

Explanation:

An external audit is an appropriate tool and technique to support a customer's verification of the cloud service provider's claims regarding its responsibilities according to the shared responsibility model. An external audit is an independent and objective examination of the cloud service provider's policies, procedures, controls, and performance by a qualified third-party auditor. An external audit can provide assurance that the cloud service provider is fulfilling its obligations and meeting the customer's expectations in terms of security, compliance, availability, reliability, and quality. An external audit can also identify any gaps or weaknesses in the cloud service provider's security posture and suggest recommendations for improvement.

An external audit can be based on various standards, frameworks, and regulations that are relevant to the cloud service provider's industry and domain. For example, some common external audits for cloud service providers are:

ISO/IEC 27001: This is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive information so that it remains secure. An ISO/IEC 27001 certification demonstrates that the cloud service provider has implemented a comprehensive and effective ISMS that covers all aspects of information security, including risk assessment, policy development, asset management, access control, incident management, business continuity, and compliance.1

SOC 2: This is an attestation report that evaluates the cloud service provider's security controls based on the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria. The Trust Services Criteria are a set of principles and criteria for evaluating the design and operating effectiveness of controls that affect the security, availability, processing integrity, confidentiality, and privacy of a system. A SOC 2 report provides assurance that the cloud service provider has implemented adequate controls to protect the customer's data and systems.2

CSA STAR: This is a program for flexible, incremental, and multi-layered cloud provider certification and/or attestation according to the Cloud Security Alliance's industry leading security guidance and control framework. The CSA STAR program consists of three levels of assurance: Level 1: SelfAssessment, Level 2: Third-Party Audit, and Level 3: Continuous Auditing. The CSA STAR program aims to provide transparency, assurance, and trust in the cloud ecosystem by enabling customers to assess and compare the security and compliance posture of cloud service providers.3

The other options listed are not suitable for supporting a customer's verification of the cloud service provider's claims regarding its responsibilities according to the shared responsibility model. An internal audit is an audit conducted by the cloud service provider itself or by an internal auditor hired by the cloud service provider. An internal audit may not be as independent or objective as an external audit, and it may not provide sufficient evidence or credibility to the customer. A contractual agreement is a legal document that defines the roles, responsibilities, expectations, and obligations

of both the cloud service provider and the customer. A contractual agreement may specify the terms and conditions for service delivery, performance, availability, security, compliance, data protection, incident response, dispute resolution, liability, and termination. However, a contractual agreement alone does not verify or validate whether the cloud service provider is actually fulfilling its claims or meeting its contractual obligations. A security assessment is a process of identifying, analyzing, and evaluating the security risks and vulnerabilities of a system or an organization. A security assessment may involve various methods such as vulnerability scanning, penetration testing, threat modeling, or risk analysis. A security assessment may provide useful information about the current state of security of a system or an organization, but it may not cover all aspects of the shared responsibility model or provide assurance that the cloud service provider is complying with its responsibilities on an ongoing basis.

Question: 53

Which of the following is a category of trust in cloud computing?

A. Loyalty-based trust
B. Background-based trust
C. Reputation-based trust
D. Transparency-based trust

Answer: C

Explanation:

Reputation-based trust is a category of trust in cloud computing that relies on the feedback, ratings, reviews, or recommendations of other users or third parties who have used or evaluated the cloud service provider or the cloud service. Reputation-based trust reflects the collective opinion and experience of the cloud community regarding the quality, reliability, security, and performance of the cloud service provider or the cloud service. Reputation-based trust can help potential customers to make informed decisions about choosing a cloud service provider or a cloud service based on the reputation score or ranking of the provider or the service. Reputation-based trust can also motivate cloud service providers to improve their services and maintain their reputation by meeting or exceeding customer expectations.

Reputation-based trust is one of the most common and widely used forms of trust in cloud computing, as it is easy to access and understand. However, reputation-based trust also has some limitations and challenges, such as:

The accuracy and validity of the reputation data may depend on the source, method, and frequency of data collection and aggregation. For example, some reputation data may be outdated, incomplete, biased, manipulated, or falsified by malicious actors or competitors.

The interpretation and comparison of the reputation data may vary depending on the context, criteria, and preferences of the customers. For example, some customers may value different aspects of the cloud service more than others, such as security, availability, cost, or functionality.

The trustworthiness and accountability of the reputation system itself may be questionable. For example, some reputation systems may lack transparency, consistency, or standardization in their design, implementation, or operation.

Therefore, reputation-based trust should not be the only factor for trusting a cloud service provider or a cloud service. Customers should also consider other forms of trust in cloud computing, such as evidence-based trust, policy-based trust, or certification-based trust

Question: 54

When establishing cloud governance, an organization should FIRST test by migrating:

A. legacy applications to the cloud.
B. a few applications to the cloud.
C. all applications at once to the cloud.
D. complex applications to the cloud

Answer: B

Explanation:

When establishing cloud governance, an organization should first test by migrating a few applications to the

cloud. Cloud governance is the process of defining and implementing policies, procedures, standards, and controls to ensure the effective, efficient, secure, and compliant use of cloud services. Cloud governance requires a clear understanding of the roles, responsibilities, expectations, and objectives of both the cloud service provider and the cloud customer, as well as the alignment of the cloud strategy with the business strategy. Cloud governance also involves monitoring, measuring, and reporting on the performance, availability, security, compliance, and cost of cloud services.

Migrating a few applications to the cloud can help an organization to test and validate its cloud governance approach before scaling up to more complex or critical applications. Migrating a few applications can also help an organization to:

Identify and prioritize the business requirements, risks, and benefits of moving to the cloud. Assess the readiness, suitability, and compatibility of the applications for the cloud.

Choose the appropriate cloud service model (such as SaaS, PaaS, or IaaS) and deployment model (such as public, private, hybrid, or multi-cloud) for each application.

Define and implement the necessary security, compliance, privacy, and data protection measures for each application.

Establish and enforce the roles and responsibilities of the cloud governance team and other stakeholders involved in the migration process.

Develop and execute a migration plan that includes testing, validation, verification, and rollback procedures for each application.

Monitor and measure the performance, availability, security, compliance, and cost of each application in the cloud.

Collect feedback and lessons learned from the migration process and use them to improve the cloud governance approach.

Migrating a few applications to the cloud can also help an organization to avoid some common pitfalls and challenges of cloud migration, such as:

Migrating legacy or incompatible applications that require significant re-engineering or refactoring to work in the cloud.

Migrating all applications at once without proper planning, testing, or governance, which can result in operational disruptions, data loss, security breaches, or compliance violations.

Migrating complex or critical applications without adequate testing or governance, which can increase the risk of failure or downtime.

Migrating applications without considering the impact on the end-users or customers, who may experience changes in functionality, performance, usability, or accessibility.

Therefore, migrating a few applications to the cloud is a recommended best practice for establishing cloud governance. It can help an organization to gain experience and confidence in using cloud services while ensuring that its cloud governance approach is effective, efficient, secure, and compliant.

Reference:

Migration environment planning checklist - Cloud Adoption Framework

Cloud Governance: What You Need To Know - Forbes

Cloud Governance: A Comprehensive Guide - BMC Blogs

Question: 55

Which of the following methods can be used by a cloud service provider with a cloud customer that does not want to share security and control information?

A. Nondisclosure agreements (NDAs)

B. Independent auditor report
C. First-party audit
D. Industry certifications

Answer: B

Explanation:
An independent auditor report is a method that can be used by a cloud service provider (CSP) with a cloud customer that does not want to share security and control information. An independent auditor report is a document that provides assurance on the CSP's security and control environment, based on an audit conducted by a qualified third-party auditor. The audit can be based on various standards or frameworks, such as ISO 27001, SOC 2, CSA STAR, etc. The independent auditor report can provide the cloud customer with the necessary information to evaluate the CSP's security and control posture, without disclosing sensitive or proprietary details. The CSP can also use the independent auditor report to demonstrate compliance with relevant regulations or contractual obligations.

Reference:
ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 83-84.
ISACA, Cloud Computing Audit Program, 2019, p. 6-7.

Question: 56

Application programming interfaces (APIs) are likely to be attacked continuously by bad actors because they:

A. are the asset with private IP addresses.
B. are generally the most exposed part.
C. could be poorly designed.
D. act as a very effective backdoor.

Answer: B

Explanation:
APIs are likely to be attacked continuously by bad actors because they are generally the most exposed part of an application or system. APIs serve as the interface between different components or services, and often expose sensitive data or functionality to the outside world. APIs can be accessed by anyone with an Internet connection, and can be easily discovered by scanning or crawling techniques. Therefore, APIs are a prime target for attackers who want to exploit vulnerabilities, steal data, or disrupt services.

Reference:
ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 88-89.
OWASP, The Ten Most Critical API Security Risks - OWASP Foundation, 2019, p. 4-5

Question: 57

In a multi-level supply chain structure where cloud service provider A relies on other sub cloud services, the provider should ensure that any compliance requirements relevant to the provider are:

A. treated as confidential information and withheld from all sub cloud service providers.
B. treated as sensitive information and withheld from certain sub cloud service providers.
C. passed to the sub cloud service providers.

D. passed to the sub cloud service providers based on the sub cloud service providers' geographic location.

Answer: C

Explanation:
In a multi-level supply chain structure where cloud service provider A relies on other sub cloud service providers, the provider should ensure that any compliance requirements relevant to the provider are passed to the sub cloud service providers. This is because the sub cloud service providers may have access to or process the provider's data or resources, and therefore need to comply with the same standards and regulations as the provider. Passing the compliance requirements to the sub cloud service providers can also help the provider to monitor and audit the sub cloud service providers' performance and security, and to mitigate any risks or issues that may arise.

Reference:
ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 85-86.
CSA, Cloud Controls Matrix (CCM) v4.0, 2021, p. 7-8

Question: 58

Which of the following cloud service provider activities MUST obtain a client's approval?

A. Destroying test data
B. Deleting subscription owner accounts
C. Deleting test accounts
D. Deleting guest accounts

Answer: B

Explanation:
Deleting subscription owner accounts is an activity that MUST obtain a client's approval in the context of cloud service provider activities. Subscription owner accounts are critical as they hold the ownership and control over the resources and services within a cloud subscription. Deleting these accounts can have significant implications, including loss of access, control, and potential data loss. Therefore, it is essential for a cloud service provider to seek explicit approval from the client before proceeding with such an action to ensure transparency, maintain trust, and avoid any unintended consequences.

Reference:
Microsoft Trust Center, Cloud Services Due Diligence Checklist1.
Google Cloud, What is a Cloud Service Provider?2.
Partner Center, CSP agreements, price lists, and offers3.
Microsoft Azure, How to choose a cloud service provider4.
FCA, FG16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services

Question: 59

A contract containing the phrase "You automatically consent to these terms by using or logging into the service to which they pertain" is establishing a contract of:

A. exclusivity.
B. adhesion.
C. execution.

D. exclusion.

Answer: B

Explanation:
A contract containing the phrase "You automatically consent to these terms by using or logging into the service to which they pertain" is establishing a contract of adhesion. A contract of adhesion is a type of legal agreement that involves one party setting the terms and conditions and the other party having no choice but to accept or reject them without bargaining. These contracts are often used in situations where one party has more power or resources than the other, such as in online services, insurance, leases, or consumer credit. These contracts may be unfair or unclear to the weaker party and may be challenged in court for unconscionability or ambiguity12.

Reference:
adhesion contract | Wex | US Law | LII / Legal Information Institute
What is a contract of adhesion? A complete guide - PandaDoc

Question: 60

Regarding cloud service provider agreements and contracts, unless otherwise stated, the provider is:

A. responsible to the cloud customer and its clients.
B. responsible only to the cloud customer.
C. not responsible at all to any external parties.
D. responsible to the cloud customer and its end users

Answer: B

Explanation:
Regarding cloud service provider agreements and contracts, unless otherwise stated, the provider is responsible only to the cloud customer. This means that the provider has a contractual obligation to deliver the agreed-upon services and meet the service level agreements (SLAs) with the cloud customer, who is the direct payer of the services. The provider is not responsible for any other parties, such as the cloud customer's clients, end users, or regulators, unless explicitly specified in the contract. The cloud customer is responsible for ensuring that the provider's services meet their own compliance and security requirements, as well as those of their stakeholders12.

Reference:
Shared responsibility in the cloud - Microsoft Azure
Cloud security shared responsibility model - NCSC

Question: 61

A cloud service provider contracts for a penetration test to be conducted on its infrastructures. The auditor engages the target with no prior knowledge of its defenses, assets, or channels. The provider's security operation center is not notified in advance of the scope of the audit and the test vectors. Which mode has been selected by the provider?

A. Reversal
B. Double blind

C. Double gray box

D. Tandem

Answer: B

Explanation:

A double blind penetration test is a type of pen test where the hacker has no prior knowledge of the target's defenses, assets, or channels, and the target's security team is not notified in advance of the scope of the audit and the test vectors. This mode simulates a real-world attack scenario, where both the attacker and the defender have to rely on their skills and resources to achieve their objectives. A double blind penetration test can help evaluate the effectiveness of the target's security posture, detection and response capabilities, and incident management procedures12.

Reference:

What is Penetration Testing | Step-By-Step Process & Methods | Imperva

7 Types of Penetration Testing: Guide to Pentest Methods & Types

Question: 62

In the context of Infrastructure as a Service (IaaS), a vulnerability assessment will scan virtual machines to identify vulnerabilities in:

A. both operating system and application infrastructure contained within the cloud service provider's instances.

B. both operating system and application infrastructure contained within the customer's instances.

C. only application infrastructure contained within the cloud service provider's instances.

D. only application infrastructure contained within the customer's instance

Answer: B

Explanation:

In the context of Infrastructure as a Service (IaaS), a vulnerability assessment will scan virtual machines to identify vulnerabilities in both operating system and application infrastructure contained within the customer's instances. IaaS is a cloud service model that provides customers with access to virtualized computing resources, such as servers, storage, and networks, hosted by a cloud service provider (CSP). The customer is responsible for installing, configuring, and maintaining the operating system and application software on the virtual machines, while the CSP is responsible for managing the underlying physical infrastructure. Therefore, a vulnerability assessment will scan the customer's instances to detect any weaknesses or misconfigurations in the operating system and application layers that may expose them to potential threats. A vulnerability assessment can help the customer to prioritize and remediate the identified vulnerabilities, and to comply with relevant security standards and regulations12.

Reference:

Azure Security Control - Vulnerability Management | Microsoft Learn

How to Implement Enterprise Vulnerability Assessment - Gartner

Question: 63

The Cloud Octagon Model was developed to support organizations':

A. risk treatment methodology.
B. incident detection methodology.
C. incident response methodology.
D. risk assessment methodology.

Answer: D

Explanation:
The Cloud Octagon Model was developed to support organizations' risk assessment methodology. Risk assessment is the process of identifying, analyzing, and evaluating the risks associated with a cloud computing environment. The Cloud Octagon Model provides a logical approach to holistically deal with security aspects involved in moving to the cloud by introducing eight dimensions that need to be considered: procurement, IT governance, architecture, development and engineering, service providers, risk processes, data classification, and country. The model aims to reduce risks, improve effectiveness, manageability, and security of cloud solutions12.

Reference:
Cloud Octagon Model | CSA
Cloud Security Alliance Releases Cloud Octagon Model

Question: 64

When an organization is moving to the cloud, responsibilities are shared based upon the cloud service provider's model and accountability is:

A. shared.
B. avoided.
C. transferred.
D. maintained.

Answer: D

Explanation:
When an organization is moving to the cloud, responsibilities are shared based upon the cloud service provider's model and accountability is maintained. This means that the organization remains accountable for the security and compliance of its data and applications in the cloud, even if some of the security responsibilities are delegated to the cloud service provider (CSP). The organization cannot transfer or avoid its accountability to the CSP or any other third party, as it is ultimately responsible for its own business outcomes, legal obligations, and reputation. Therefore, the organization must understand the shared responsibility model and which security tasks are handled by the CSP and which tasks are handled by itself. The organization must also monitor and audit the CSP's performance and security, and mitigate any risks or issues that may arise12.

Reference:
Shared responsibility in the cloud - Microsoft Azure
Understanding the Shared Responsibilities Model in Cloud Services - ISACA

Question: 65

Which of the following is the MOST relevant question in the cloud compliance program design phase?

A. Who owns the cloud services strategy?
B. Who owns the cloud strategy?
C. Who owns the cloud governance strategy?
D. Who owns the cloud portfolio strategy?

Answer: B

Explanation:
The most relevant question in the cloud compliance program design phase is who owns the cloud governance strategy. Cloud governance is a method of information and technology (I&T) governance focused on accountability, defining decision rights and balancing benefit, risk and resources in an environment that embraces cloud computing. Cloud governance creates business-driven policies and principles that establish the appropriate degree of investments and control around the life cycle process for cloud computing services1. Therefore, it is essential to identify who owns the cloud governance strategy in the organization, as this will determine the roles and responsibilities, decision-making authority, reporting structure, and escalation process for cloud compliance

issues. The cloud governance owner should be a senior executive who has the vision, influence, and resources to drive the cloud compliance program and align it with the business objectives2. Reference:
Building Cloud Governance From the Basics - ISACA
[Cloud Governance | Microsoft Azure]

Question: 66

The MOST important factor to consider when implementing cloud-related controls is the:

A. shared responsibility model.
B. effectiveness of the controls.
C. risk reporting.
D. risk ownership

Answer: A

Explanation:
The most important factor to consider when implementing cloud-related controls is the shared responsibility model. The shared responsibility model is a framework that defines the roles and responsibilities of cloud service providers (CSPs) and cloud customers (CCs) in ensuring the security and compliance of cloud computing environments. The shared responsibility model helps to clarify which security tasks are handled by the CSP and which tasks are handled by the CC, depending on the type of cloud service model (IaaS, PaaS, SaaS) and the specific contractual agreements. The shared responsibility model also helps to avoid gaps or overlaps in security controls, and to allocate resources and accountability accordingly12.
Reference:
Shared responsibility in the cloud - Microsoft Azure
Understanding the Shared Responsibilities Model in Cloud Services - ISACA

Question: 67

Which of the following has the MOST substantial impact on how aggressive or conservative the cloud approach of an organization will be?

A. Applicable laws and regulations
B. Internal policies and technical standards
C. Risk scoring criteria
D. Risk appetite and budget constraints

Answer: D

Explanation:

Risk appetite and budget constraints have the most substantial impact on how aggressive or conservative the cloud approach of an organization will be. Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Budget constraints are the limitations on the financial resources that an organization can allocate to its cloud initiatives. Both

factors influence the organization's strategic decisions on which cloud service models, deployment models, providers, and solutions to adopt, as well as the level of security, compliance, and performance to achieve. An organization with a high risk appetite and a large budget may opt for a more aggressive cloud approach, such as moving critical applications and data to a public cloud provider, while an organization with a low risk appetite and a small budget may opt for a more conservative cloud approach, such as keeping sensitive information on-premises or using a private cloud provider12.

Reference:

ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 17-18.

CSA, Cloud Controls Matrix (CCM) v4.0, 2021, p. 63.

Question: 68

When developing a cloud compliance program, what is the PRIMARY reason for a cloud customer

A. To determine the total cost of the cloud services to be deployed
B. To confirm whether the compensating controls implemented are sufficient for the cloud services
C. To determine how those services will fit within its policies and procedures
D. To confirm which vendor will be selected based on compliance with security requirements

Answer: C

Explanation:

When developing a cloud compliance program, the primary reason for a cloud customer to determine how those services will fit within its policies and procedures is to ensure that the cloud services are aligned with the customer's business objectives, risk appetite, and compliance obligations. Cloud services may have different characteristics, features, and capabilities than traditional on-premises services, and may require different or additional controls to meet the customer's security and compliance requirements. Therefore, the customer needs to assess how the cloud services will fit within its existing policies and procedures, such as data classification, data protection, access management, incident response, audit, and reporting. The customer also needs to identify any gaps or conflicts between the cloud services and its policies and procedures, and implement appropriate measures to address them. By doing so, the customer can ensure that the cloud

services are used in a secure, compliant, and effective manner12.

Reference:

ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 19-20.

Cloud Compliance Frameworks: What You Need to Know

Question: 69

A new company has all its operations in the cloud. Which of the following would be the BEST information security control framework to implement?

A. NIST 800-73, because it is a control framework implemented by the main cloud providers

B. ISO/IEC 27018

C. ISO/IEC 27002

D. (S) Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Answer: D

Explanation:

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) would be the best information security control framework to implement for a new company that has all its operations in the cloud. The CCM is a cybersecurity control framework for cloud computing that is aligned to the CSA best practices and is considered the de-facto standard for cloud security and privacy. The CCM covers 17 domains and 197 control objectives that address all key aspects of cloud technology, such as data security, identity and access management, encryption and key management, incident response, audit assurance, and compliance. The CCM also maps to other industry-accepted security standards, regulations, and frameworks, such as ISO 27001/27002/27017/27018, NIST SP 800-53, PCI DSS, COBIT, FedRAMP, etc., which can help the company to achieve multiple compliance goals with one framework. The CCM also provides guidance on the shared responsibility model between cloud service providers and cloud customers, and helps to define the organizational relevance of each control12.

Reference:

Cloud Controls Matrix (CCM) - CSA

Cloud Controls Matrix and CAIQ v4 | CSA - Cloud Security Alliance

Question: 70

Which of the following processes should be performed FIRST to properly implement the NIST SP 80053 r4 control framework in an organization?

A. A selection of the security objectives the organization wants to improve

B. A security categorization of the information systems

C. A comprehensive business impact analysis (BIA)

D. A comprehensive tailoring of the controls of the framework

Answer: B

Explanation:

A security categorization of the information systems should be performed first to properly implement the NIST SP 800-53 r4 control framework in an organization. Security categorization is the process of determining the

potential impact on organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from a loss of confidentiality, integrity, or availability of an information system and the information processed, stored, or transmitted by that system. Security categorization is based on the application of FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, which defines three levels of impact: low, moderate, and high. Security categorization is the first step in the Risk Management Framework (RMF) described in NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

Security categorization helps to identify the security requirements for the information system and to select an initial set of baseline security controls from NIST SP 800-53 r4, Security and Privacy Controls for Federal Information Systems and Organizations. The baseline security controls can then be

tailored and supplemented as needed to address specific organizational needs, risk factors, and compliance obligations12.

Reference:

SP 800-53 Rev. 4, Security & Privacy Controls for Federal Info Sys …

SP 800-37 Rev. 2, Risk Management Framework for Information …

Question: 71

Which of the following enables auditors to conduct gap analyses of what a cloud service provider offers versus what the customer requires?

A. Using a standardized control framework
B. The experience gained over the years
C. Understanding the customer risk profile
D. The as-is and to-be enterprise architecture (EA

Answer: A

Explanation:

Using a standardized control framework enables auditors to conduct gap analyses of what a cloud service provider (CSP) offers versus what the customer requires. A standardized control framework is a set of guidelines, best practices, and criteria that help to evaluate and improve the security, privacy, and compliance of cloud computing environments. Examples of standardized control frameworks include ISO/IEC 27001/27002/27017/27018, NIST SP 800-53, CSA Cloud Controls Matrix (CCM), COBIT, etc. By using a standardized control framework, auditors can compare the CSP's policies, procedures, and practices with the customer's expectations and requirements, and identify any gaps or discrepancies that may pose risks or issues. A gap analysis can help the auditors to provide recommendations and suggestions to the CSP and the customer on how to close the gaps and enhance the quality and performance of the cloud services12.

Reference:

Cloud Controls Matrix (CCM) - CSA

Cloud Computing Audit Program - ISACA

Question: 72

An organization currently following the ISO/IEC 27002 control framework has been charged by a new CIO to switch to the NIST 800-53 control framework. Which ofthe following is the FIRST step to this change?

A. Discard all work done and start implementing NIST 800-53 from scratch.
B. Recommend no change, since the scope of ISO/IEC 27002 is broader.
C. Recommend no change, since NIST 800-53 is a US-scoped control framework.
D. Map ISO/IEC 27002 and NIST 800-53 and detect gaps and commonalities.

Answer: D

Explanation:

The first step to switch from the ISO/IEC 27002 control framework to the NIST 800-53 control framework is to map ISO/IEC 27002 and NIST 800-53 and detect gaps and commonalities. This step can help the organization to understand the similarities and differences between the two frameworks, and to identify which controls are already implemented, which controls need to be added or modified, and which controls are no longer applicable. Mapping can also help the organization to leverage the existing work done under ISO/IEC 27002 and avoid starting from scratch or discarding valuable information. Mapping can also help the organization to align with both frameworks, as they are not mutually exclusive or incompatible. In fact, NIST SP 800-53, Revision 5 provides a mapping table between NIST 800-53 and ISO/IEC 27001 in Appendix H-21. ISO/IEC 27001 is a standard for information security management systems that is based on ISO/IEC 27002, which is a code of practice for information security controls2.

Reference:
NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001
ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls

Question: 73

The CSA STAR Certification is based on criteria outlined the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to:

A. GDPR CoC certification.
B. GB/T 22080-2008.
C. SOC 2 Type 1 or 2 reports.
D. ISO/IEC 27001 implementation.

Answer: D

Explanation:
The CSA STAR Certification is based on criteria outlined in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) in addition to ISO/IEC 27001 implementation. The CCM is a cybersecurity control framework for cloud computing that covers 17 domains and 197 control objectives that address all key aspects of cloud technology. ISO/IEC 27001 is a standard for information security management systems that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. The CSA STAR Certification demonstrates that a cloud service provider conforms to the applicable requirements of ISO/IEC 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas1. The CSA STAR Certification is a third-party independent assessment of the security of a cloud service provider and provides a high level of assurance and trust to customers2.

Reference:

CSA STAR Certification - Azure Compliance | Microsoft Learn STAR | CSA

Question: 74

Transparent data encryption is used for:

A. data across communication channels.
B. data currently being processed.
C. data in random access memory (RAM).
D. data and log files at rest

Answer: D

Explanation:

Transparent data encryption (TDE) is used for data and log files at rest. This means that TDE encrypts the database files on the disk and decrypts them when they are read into memory. TDE protects the data from unauthorized access or theft if the physical media, such as drives or backup tapes, are stolen or lost. TDE does not encrypt data across communication channels, data currently being processed, or data in random access memory (RAM). These types of data require different encryption methods, such as SSL/TLS, column encryption, or memory encryption12.

Reference:

Transparent data encryption (TDE) - SQL Server | Microsoft Learn

Transparent Data Encryption - Oracle Help Center

Question: 75

When reviewing a third-party agreement with a cloud service provider, which of the following should be the GREATEST concern regarding customer data privacy?

A. Return or destruction of information
B. Data retention, backup, and recovery
C. Patch management process
D. Network intrusion detection

Answer: A

Explanation:

When reviewing a third-party agreement with a cloud service provider, the greatest concern regarding customer data privacy is the return or destruction of information. This is because customer data may contain sensitive or personal information that needs to be protected from unauthorized access, use, or disclosure. The cloud service provider should have clear and transparent policies and procedures for returning or destroying customer data upon termination of the agreement or upon customer request. The cloud service provider should also provide evidence of the return or destruction of customer data, such as certificates of destruction, audit logs, or reports. The return or destruction of information should comply with applicable laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the Health Insurance Portability and Accountability Act (HIPAA). The cloud service provider should also ensure that any subcontractors or affiliates that have access to customer data follow the same policies and procedures12.

Reference:
Cloud Services Agreements – Protecting Your Hosted Environment
CSP agreements, price lists, and offers - Partner Center

Question: 76

Which of the following metrics are frequently immature?

A. Metrics around specific Software as a Service (SaaS) application services
B. Metrics around Infrastructure as a Service (IaaS) computing environments
C. Metrics around Infrastructure as a Service (IaaS) storage and network environments
D. Metrics around Platform as a Service (PaaS) development environments

Answer: D

Explanation:
Metrics around Platform as a Service (PaaS) development environments are frequently immature, as PaaS is a relatively new and evolving cloud service model that offers various tools and platforms for developing, testing, deploying, and managing cloud applications. PaaS metrics are often not well- defined, standardized, or consistent across different providers and platforms, and may not capture the full value and performance of PaaS services. PaaS metrics may also be difficult to measure, monitor, and compare, as they depend on various factors, such as the type, complexity, and quality of the applications, the level of customization and integration, the usage patterns and demand, and the security and compliance requirements. Therefore, PaaS metrics may not provide sufficient insight or assurance to cloud customers and auditors on the effectiveness, efficiency, reliability, and security of PaaS services12.
Reference:
Cloud Computing Service Metrics Description - NIST
Cloud KPIs You Need to Measure Success - VMware Blogs

Question: 77

To promote the adoption of secure cloud services across the federal government by

A. To providing a standardized approach to security and risk assessment
B. To provide agencies of the federal government a dedicated tool to certify Authority to Operate (ATO)
C. To enable 3PAOs to perform independent security assessments of cloud service providers D. To publish a comprehensive and official framework for the secure implementation of controls for cloud security

Answer: A

Explanation:
The correct answer is A. To providing a standardized approach to security and risk assessment. This is the main purpose of FedRAMP, which is a government-wide program that promotes the adoption of secure cloud services across the federal government. FedRAMP provides a standardized methodology for assessing, authorizing, and monitoring the security of cloud products and services, and enables agencies to leverage the security assessments of cloud service providers (CSPs) that

have been approved by FedRAMP. FedRAMP also establishes a baseline set of security controls for cloud

computing, based on NIST SP 800-53, and provides guidance and templates for implementing and documenting the controls1.

The other options are incorrect because:

B . To provide agencies of the federal government a dedicated tool to certify Authority to Operate (ATO): FedRAMP does not provide a tool to certify ATO, but rather a process to obtain a provisional ATO (P-ATO) from the Joint Authorization Board (JAB) or an agency ATO from a federal agency. ATO is the official management decision given by a senior official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls2.

C . To enable 3PAOs to perform independent security assessments of cloud service providers: FedRAMP does not enable 3PAOs to perform independent security assessments of CSPs, but rather requires CSPs to use 3PAOs for conducting independent security assessments as part of the FedRAMP process. 3PAOs are independent entities that have been accredited by FedRAMP to perform initial and periodic security assessments of CSPs' systems and provide evidence of compliance with FedRAMP requirements3.

D . To publish a comprehensive and official framework for the secure implementation of controls for cloud security: FedRAMP does not publish a comprehensive and official framework for the secure implementation of controls for cloud security, but rather adopts and adapts the existing framework of NIST SP 800-53, which provides a catalog of security and privacy controls for federal information systems and organizations. FedRAMP tailors the NIST SP 800-53 controls to provide a subset of controls that are specific to cloud computing, and categorizes them into low, moderate, and high impact levels based on FIPS 1994.

Reference:

Learn What FedRAMP is All About | FedRAMP | FedRAMP.gov
Guide for Applying the Risk Management Framework to Federal Information Systems - NIST
Third Party Assessment Organizations (3PAO) | FedRAMP.gov
Security and Privacy Controls for Federal Information Systems and Organizations - NIST

Question: 78

Which of the following has been provided by the Federal Office for Information Security in Germany to support customers in selecting, controlling, and monitoring their cloud service providers?

A. BSI IT-basic protection catalogue
B. Multi-Tier Cloud Security (MTCS)
C. German IDW PS 951
D. BSI Criteria Catalogue C5

Answer: D

Explanation:

The BSI Criteria Catalogue C5 is a document that has been provided by the Federal Office for Information Security (BSI) in Germany to support customers in selecting, controlling, and monitoring their cloud service providers (CSPs). The C5 stands for Cloud Computing Compliance Criteria Catalogue and specifies minimum requirements for secure cloud computing. The C5 is primarily intended for professional CSPs, their auditors, and customers of the CSPs. The C5 covers 17 domains and 114 control objectives that address all key aspects of cloud security, such as data protection,
identity and access management, encryption and key management, incident response, audit assurance, and compliance. The C5 also maps to other industry-accepted security standards, regulations, and frameworks, such as ISO 27001/27002/27017/27018, NIST SP 800-53, CSA Cloud Controls Matrix (CCM), COBIT, GDPR, etc.
The C5 helps customers to evaluate and compare the security and compliance posture of different CSPs, and to

verify that the CSPs meet their contractual obligations and legal requirements12.

Reference:

BSI - C5 criteria catalogue - Federal Office for Information Security

Germany C5 - Azure Compliance | Microsoft Learn

Question: 79

A cloud service provider providing cloud services currently being used by the United States federal government should obtain which of the following to assure compliance to stringent government standards?

A. CSA STAR Level Certificate
B. Multi-Tier Cloud Security (MTCS) Attestation
C. ISO/IEC 27001:2013 Certification
D. FedRAMP Authorization

Answer: D

Explanation:

A cloud service provider (CSP) providing cloud services currently being used by the United States federal government should obtain FedRAMP Authorization to assure compliance to stringent government standards. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP enables agencies to leverage the security assessments of CSPs that have been approved by FedRAMP, and establishes a baseline set of security controls for cloud computing, based on NIST SP 800-53. FedRAMP also helps CSPs to demonstrate their compliance with relevant laws and regulations, such as FISMA, FIPS, and NIST standards. FedRAMP Authorization can be obtained through two paths: a provisional authorization from the Joint Authorization Board (JAB) or an authorization from an individual agency12.

The other options are incorrect because:

A . CSA STAR Level Certificate: CSA STAR is a program for security assurance in the cloud that encompasses key principles of transparency, rigorous auditing, and harmonization of standards. CSA STAR Level Certificate is one of the certification options offered by CSA STAR, which is based on the ISO/IEC 27001 standard and the CSA Cloud Controls Matrix (CCM). CSA STAR Level Certificate is not specific to the US federal government standards, and does not guarantee compliance with FedRAMP requirements3.

B . Multi-Tier Cloud Security (MTCS) Attestation: MTCS is a cloud security standard developed by the Singapore government to provide greater clarity and transparency on the level of security offered by different CSPs. MTCS defines three levels of security controls for CSPs: Level 1, Level 2, and Level 3, with Level 3 being the most stringent. MTCS Attestation is a voluntary self-disclosure scheme for CSPs to declare their conformance to the MTCS standard. MTCS Attestation is not applicable to the US federal government standards, and does not ensure compliance with FedRAMP requirements4. C . ISO/IEC 27001:2013 Certification: ISO/IEC 27001 is a standard for information security

management systems that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. ISO/IEC 27001 Certification is an independent verification that an organization conforms to the ISO/IEC 27001 standard. ISO/IEC 27001 Certification is not exclusive to cloud computing or the US federal government standards, and does not cover all aspects of FedRAMP requirements5.

Reference:

Learn What FedRAMP is All About | FedRAMP | FedRAMP.gov

How to Become FedRAMP Authorized | FedRAMP.gov

STAR | CSA
Multi-Tiered Cloud Security Standard (MTCS SS)
ISO - ISO/IEC 27001 — Information security management

Question: 80

A dot release of the Cloud Controls Matrix (CCM) indicates:

A. a revision of the CCM domain structure.
B. a technical change (revision, addition, or deletion) of a number of controls that is smaller than 10% compared to the previous full release.
C. the introduction of new control frameworks mapped to previously published CCM controls.
D. technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release.

Answer: B

Explanation:
A dot release of the Cloud Controls Matrix (CCM) indicates a technical change (revision, addition, or deletion) of a number of controls that is smaller than 10% compared to the previous full release. A dot release is a minor update to the CCM that reflects the feedback from the cloud security community and the changes in the cloud technology landscape. A dot release does not change the domain structure or the overall scope of the CCM, but rather improves the clarity, accuracy, and relevance of the existing controls. A dot release is denoted by a decimal number after the major version number, such as CCM v4.1 or CCM v4.2. The current version of the CCM is v4.0, which was released in October 20211.
The other options are incorrect because:
A . a revision of the CCM domain structure: A revision of the CCM domain structure is a major change that affects the organization and categorization of the controls into different domains. A revision of the CCM domain structure requires a full release, not a dot release, and is denoted by an integer number, such as CCM v3 or CCM v42.
C . the introduction of new control frameworks mapped to previously published CCM controls: The introduction of new control frameworks mapped to previously published CCM controls is an additional feature that enhances the usability and applicability of the CCM. The introduction of new control frameworks mapped to previously published CCM controls does not require a dot release or a full release, but rather an update to the mapping table that shows the relationship between the CCM controls and other industry-accepted security standards, regulations, and frameworks3.
D . technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release: A technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release is a significant change that affects the content and scope of the CCM. A technical change (revision, addition, or deletion) of a number of controls that is greater than 10% compared to the previous full release requires a full release, not a dot release, and is denoted by an integer number, such as CCM v3 or CCM v42.
Reference:
Cloud Controls Matrix (CCM) - CSA
The CSA Cloud Controls Matrix (CCM) V4: Raising the cloud security bar
Cloud Security Alliance Releases New Cloud Controls Matrix Auditing Guidelines

Question: 81

Cloud Controls Matrix (CCM) controls can be used by cloud customers to:

A. develop new security baselines for the industry.
B. define different control frameworks for different cloud service providers.
C. build an operational cloud risk management program.
D. facilitate communication with their legal department.

Answer: C

Explanation:
The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing that can be used by cloud customers to build an operational cloud risk management program. The CCM provides guidance on which security controls should be implemented by which actor within the cloud supply chain, and maps the controls to industry-accepted security standards, regulations, and frameworks. The CCM can help cloud customers to assess the security posture of their cloud service providers, document their own responsibilities and requirements, and establish a baseline for cloud security assurance and compliance. Reference := Cloud Controls Matrix (CCM) - CSA1
What is the Cloud Controls Matrix (CCM)? - Cloud Security Alliance2
Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 5: Cloud Assurance Frameworks

Question: 82

Which of the following should a cloud auditor recommend regarding controls for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse?

A. Assessment of contractual and regulatory requirements for customer access
B. Establishment of policies and procedures across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction
C. Data input and output integrity routines
D. Testing in accordance with leading industry standards such as OWASP

Answer: C

Explanation:
The correct answer is C. Data input and output integrity routines (i.e., reconciliation and edit checks) are controls that can be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. This is stated in the Cloud Controls Matrix (CCM) control AIS-03: Data Integrity123, which is part of the Application & Interface Security domain. The CCM is a cybersecurity control framework for cloud computing that can be used by cloud customers to build an operational cloud risk management program.
The other options are not directly related to the question. Option A refers to the CCM control AIS-02: Customer Access Requirements2, which addresses the security, contractual, and regulatory requirements for customer access to data, assets, and information systems. Option B refers to the CCM control AIS-04: Data Security / Integrity2, which establishes policies and procedures to support data security across multiple system interfaces, jurisdictions, and business functions. Option D refers to the CCM control AIS-01: Application Security2, which requires applications and programming interfaces (APIs) to be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications).

Reference :=

Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 5: Cloud Assurance Frameworks
What is the Cloud Controls Matrix (CCM)? - Cloud Security Alliance4
AIS-03: Data Integrity - CSF Tools - Identity Digital1
AIS: Application & Interface Security - CSF Tools - Identity Digital2
PR.DS-6: Integrity checking mechanisms are used to verify software ... - CSF Tools - Identity Digital

Question: 83

"Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls." Which of the following types of controls BEST matches this control description?

A. Virtual instance and OS hardening
B. Network security
C. Network vulnerability management
D. Change detection

Answer: B

Explanation:
The correct answer is B. Network security is the type of control that best matches the control description given in the question. Network security involves designing and configuring network environments and virtual instances to restrict and monitor traffic between trusted and untrusted connections, such as firewalls, routers, switches, VPNs, and network segmentation. Network security also requires periodic reviews and documentation of the network configurations and the justification for the allowed services, protocols, ports, and compensating controls.
The other options are not directly related to the question. Option A, virtual instance and OS hardening, refers to the process of applying security configurations and patches to virtual instances and operating systems to reduce their attack surface and vulnerabilities. Option C, network vulnerability management, refers to the process of identifying, assessing, prioritizing, and remediating network vulnerabilities using tools such as scanners, analyzers, and testers. Option D, change detection, refers to the process of monitoring and detecting changes in the system or network environment that could affect the security posture or performance of the system or network.
Reference :=
IVS-01: Network Security - CSF Tools - Identity Digital1
Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 6: Cloud Security Controls Cloud Controls Matrix (CCM) - CSA2

Question: 84

A cloud auditor observed that just before a new software went live, the librarian transferred production data to the test environment to confirm the new software can work in the production environment. What additional control should the cloud auditor check?

A. Approval of the change by the change advisory board

B. Explicit documented approval from all customers whose data is affected
C. Training for the librarian
D. Verification that the hardware of the test and production environments are compatible

Answer: B

Explanation:
The cloud auditor should check if there is explicit documented approval from all customers whose data is affected by the transfer of production data to the test environment. This is because production data may contain sensitive or personal information that is subject to privacy and security regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). Therefore, using production data for testing purposes without the consent of the data owners may violate their rights and expose the organization to legal and reputational risks. This is also stated in the Cloud Controls Matrix (CCM) control DSI-04: Production / Non-Production Environments12, which is part of the Data Security & Information Lifecycle Management domain. The CCM is a cybersecurity control framework for cloud computing that can be used by cloud customers to build an operational cloud risk management program.
The other options are not directly related to the question. Option A, approval of the change by the change advisory board, refers to the process of reviewing and authorizing changes to the system or software before they are implemented in the production environment. This is a good practice for ensuring the quality and reliability of the system or software, but it does not address the issue of using production data for testing purposes. Option C, training for the librarian, refers to the process of providing adequate education and awareness to the staff who are responsible for managing and transferring data between different environments. This is a good practice for ensuring the competence and accountability of the staff, but it does not address the issue of obtaining consent from the data owners. Option D, verification that the hardware of the test and production environments are compatible, refers to the process of ensuring that the system or software can run smoothly and consistently on both environments. This is a good practice for ensuring the performance and functionality of the system or software, but it does not address the issue of protecting the privacy and security of the production data. Reference :=
Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, Chapter 6: Cloud Security Controls
Cloud Controls Matrix (CCM) - CSA3
DSI-04: Production / Non-Production Environments - CSF Tools - Identity Digital1
DSI: Data Security & Information Lifecycle Management - CSF Tools - Identity Digital

Question: 85

Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include:

A. regulatory guidelines impacting the cloud customer.
B. audits, assessments, and independent verification of compliance certifications with agreement terms.
C. policies and procedures of the cloud customer
D. the organizational chart of the provider.

Answer: B

Explanation:
Supply chain agreements between a cloud service provider and cloud customers should, at a minimum, include audits, assessments, and independent verification of compliance certifications with agreement terms. This is because cloud customers need to ensure that the cloud service provider meets the agreed-upon service levels,

security standards, and regulatory requirements. Audits, assessments, and independent verification can provide evidence of the cloud service provider's compliance and performance and help identify any gaps or risks that need to be addressed. This is also stated in the Practical Guide to Cloud Service Agreements Version 2.012, which is a reference document for cloud customers and providers to analyze and negotiate cloud service agreements.

The other options are not directly related to the question. Option A, regulatory guidelines impacting the cloud customer, refers to the legal and ethical obligations that the cloud customer has to comply with when using cloud services, such as data protection, privacy, and security laws. These guidelines may vary depending on the jurisdiction, industry, and type of data involved. Option C, policies and procedures of the cloud customer, refers to the internal rules and processes that the cloud customer has to follow when using cloud services, such as data governance, access management, and incident response. Option D, the organizational chart of the provider, refers to the structure and hierarchy of the cloud service provider's organization, such as the roles, responsibilities, and relationships of its employees, departments, and units.

Reference :=

Practical Guide to Cloud Service Agreements Version 2.01

Practical Guide to Cloud Service Agreements V2.0| Object ... - OMG3 Supply chain agreements between CSP and cloud customers should ...4 Practical Guide to Cloud Service Agreements Version 3

Question: 86

Which of the following is the reason for designing the Consensus Assessments Initiative Questionnaire (CAIQ)?

A. Cloud users can use CAIQ to sign statement of work (SOW) with cloud access security brokers (CASBs).
B. Cloud service providers can document roles and responsibilities for cloud security.
C. Cloud service providers can document their security and compliance controls.
D. Cloud service providers need the CAIQ to improve quality of customer service

Answer: C

Explanation:

The reason for designing the Consensus Assessments Initiative Questionnaire (CAIQ) is to help cloud service providers document their security and compliance controls. The CAIQ is a survey provided by the Cloud Security Alliance (CSA) that consists of a set of yes/no questions that correspond to the controls of the Cloud Controls Matrix (CCM), which is a cybersecurity framework for cloud computing. The CAIQ allows cloud service providers to demonstrate their security posture and compliance status to potential customers and auditors, as well as to identify any gaps or risks that need to be addressed. The CAIQ also enables cloud customers to assess the security capabilities of different cloud service providers and compare them based on their needs and requirements123. The other options are not directly related to the question. Option A, cloud users can use CAIQ to sign statement of work (SOW) with cloud access security brokers (CASBs), is incorrect because CAIQ is not a contract or an agreement, but a questionnaire that provides information about the security controls of a cloud service provider. A statement of work (SOW) is a document that defines the scope, deliverables, and terms of a project or service. A cloud access security broker (CASB) is a software tool or service that acts as an intermediary between cloud users and cloud service providers, providing visibility, data security, threat protection, and compliance4. Option B, cloud service providers can document roles and responsibilities for cloud security, is incorrect because CAIQ is not designed to document roles and responsibilities, but security and compliance controls. Roles and responsibilities for cloud security are defined by the shared responsibility model, which outlines how the security tasks and obligations are divided between the cloud service provider and the cloud customer5. Option D, cloud service providers need the CAIQ to improve quality of customer

service, is incorrect because CAIQ is not a measure of customer service quality, but a measure of security control transparency. Customer service quality refers to how well a cloud service provider meets or exceeds the expectations and satisfaction of its customers6. Reference := What is CASB? - Cloud Security Alliance4

What is CAIQ? | CSA - Cloud Security Alliance1

Shared Responsibility Model - Cloud Security Alliance5

What is CAIQ? - Panorays2

What is the Consensus Assessments Initiative Questionnaire (CAIQ ...3

What Is Customer Service Quality? - Salesforce.com

Question: 87

An organization is using the Cloud Controls Matrix (CCM) to extend its IT governance in the cloud. Which of the following is the BEST way for the organization to take advantage of the supplier relationship feature?

A. Filter out only those controls directly influenced by contractual agreements.
B. Leverage this feature to enable the adoption of the Shared Responsibility Model.
C. Filter out only those controls having a direct impact on current terms of service (TOS) and service level agreement (SLA).
D. Leverage this feature to enable a smarter selection of the next cloud provider.

Answer: D

Explanation:
The best way for the organization to take advantage of the supplier relationship feature of the Cloud Controls Matrix (CCM) is to leverage this feature to enable a smarter selection of the next cloud provider. The supplier relationship feature is a column in the CCM spreadsheet that indicates whether a control is influenced by contractual agreements between the cloud service provider and the cloud customer. This feature can help the organization to identify and compare the security and compliance capabilities of different cloud providers, as well as to negotiate and customize the terms of service (TOS) and service level agreements (SLA) according to their needs and requirements123. The other options are not the best ways to use the supplier relationship feature. Option A, filter out only those controls directly influenced by contractual agreements, is not a good way to use the feature because it would exclude other important controls that are not influenced by contractual agreements, but still relevant for cloud security and governance. Option B, leverage this feature to enable the adoption of the Shared Responsibility Model, is not a good way to use the feature because the Shared Responsibility Model is defined by another column in the CCM spreadsheet, which indicates whether a control is applicable to the cloud service provider or the cloud customer. Option C, filter out only those controls having a direct impact on current TOS and SLA, is not a good way to use the feature because it would exclude other controls that may have an indirect or potential impact on the TOS and SLA, or that may be subject to change or negotiation in the future. Reference :=
What is CAIQ? | CSA - Cloud Security Alliance1
Understanding the Cloud Control Matrix | CloudBolt Software3
Cloud Controls Matrix (CCM) - CSA2

Question: 88

Controls mapping found in the Scope Applicability column of the Cloud Controls Matrix (CCM) may help organizations to realize cost savings:

A. by avoiding duplication of efforts in the compliance evaluation and for the eventual control design and implementation.

B. by implementing layered security, thus reducing the likelihood of data breaches and the associated costs.

C. by avoiding the need to hire a cloud security specialist to perform the periodic risk assessment exercise.

D. by avoiding fines for breaching those regulations that impose a controls mapping in order to prove compliance

Answer: A

Explanation:

Controls mapping found in the Scope Applicability column of the Cloud Controls Matrix (CCM) may help organizations to realize cost savings by avoiding duplication of efforts in the compliance

evaluation and for the eventual control design and implementation. The Scope Applicability column is a feature of the CCM that indicates which cloud model type (IaaS, PaaS, SaaS) or cloud environment (public, hybrid, private) a control applies to. This feature can help organizations to identify and select the most relevant and appropriate controls for their specific cloud scenario, as well as to map them to multiple industry-accepted security standards, regulations, and frameworks. By doing so, organizations can reduce the time, resources, and costs involved in achieving and maintaining compliance with various cloud security requirements123.

The other options are not directly related to the question. Option B, by implementing layered security, thus reducing the likelihood of data breaches and the associated costs, is not a valid reason because layered security is a general principle of defense in depth, not a specific feature of the CCM or the Scope Applicability column. Option C, by avoiding the need to hire a cloud security specialist to perform the periodic risk assessment exercise, is not a valid reason because using the CCM or the Scope Applicability column does not eliminate the need for a cloud security specialist or a periodic risk assessment exercise, which are essential for ensuring the effectiveness and adequacy of the cloud security controls. Option D, by avoiding fines for breaching those regulations that impose a controls mapping in order to prove compliance, is not a valid reason because controls mapping is not a mandatory requirement for proving compliance, but a voluntary tool for facilitating compliance. Reference :=

What is CAIQ? | CSA - Cloud Security Alliance1

Understanding the Cloud Control Matrix | CloudBolt Software2

Cloud Controls Matrix (CCM) - CSA

Question: 89

When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?

A. Determine the impact on the controls that were selected by the organization to respond to identified risks.

B. Determine the impact on confidentiality, integrity, and availability of the information system.

C. Determine the impact on the physical and environmental security of the organization, excluding informational assets.

D. Determine the impact on the financial, operational, compliance, and reputation of the organization.

Answer: B

Explanation:

When applying the Top Threats Analysis methodology following an incident, the scope of the technical impact identification step is to determine the impact on confidentiality, integrity, and availability of the information system. The Top Threats Analysis methodology is a framework developed by the Cloud Security Alliance (CSA) to help organizations identify, analyze, and mitigate the most critical threats to cloud computing. The methodology consists of six steps: threat identification, threat analysis, technical impact identification, business impact analysis, risk assessment, and risk treatment12.

The technical impact identification step is the third step of the methodology, and it aims to assess how the incident affected the security properties of the information system, namely confidentiality, integrity, and availability. Confidentiality refers to the protection of data from unauthorized access or disclosure. Integrity refers to the protection of data from unauthorized modification or deletion. Availability refers to the protection of data and services from disruption or denial. The technical impact identification step can help organizations to understand the severity and extent of the incident and its consequences on the information system12.

The other options are not within the scope of the technical impact identification step. Option A, determine the impact on the controls that were selected by the organization to respond to identified risks, is not within the scope because it is part of the risk treatment step, which is the sixth and final step of the methodology. Option C, determine the impact on the physical and environmental security of the organization, excluding informational assets, is not within the scope because it is not related to the information system or its security properties. Option D, determine the impact on the financial, operational, compliance, and reputation of the organization, is not within the scope because it is part of the business impact analysis step, which is the fourth step of the methodology. Reference := Top Threats Analysis Methodology - CSA1

Top Threats Analysis Methodology - Cloud Security Alliance

Question: 90

Which of the following is an example of financial business impact?

A. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours, resulting in millions in lost sales.

B. A hacker using a stolen administrator identity brings down the Software of a Service (SaaS) sales and marketing systems, resulting in the inability to process customer orders or manage customer relationships.

C. While the breach was reported in a timely manner to the CEO, the CFO and CISO blamed each other in public consulting in a loss of public confidence that led the board to replace all three.

Answer: A

Explanation:

An example of financial business impact is a distributed denial of service (DDoS) attack that renders the customer's cloud inaccessible for 24 hours, resulting in millions in lost sales. Financial business impact refers to the monetary losses or gains that an organization may experience as a result of a cloud security incident. Financial business impact can be measured by factors such as revenue, profit, cost, cash flow, market share, and stock price .

Option A is an example of financial business impact because it shows how a DDoS attack, which is a type of cyberattack that overwhelms a system or network with malicious traffic and prevents legitimate users from accessing it, can cause direct and significant financial losses for the customer's organization due to the

interruption of its cloud services and the inability to generate sales. Option A also implies that the customer's organization depends on the availability of its cloud services for its core business operations.
The other options are not examples of financial business impact. Option B is an example of operational business impact, which refers to the disruption or degradation of the organization's processes, functions, or activities as a result of a cloud security incident. Operational business impact can be measured by factors such as productivity, efficiency, quality, performance, and customer satisfaction . Option B shows how a hacker using a stolen administrator identity, which is a type of

identity theft or impersonation attack that exploits the credentials or privileges of a legitimate user to access or manipulate a system or network, can cause operational business impact for the customer's organization by bringing down its SaaS sales and marketing systems, which are essential for its business functions.
Option C is an example of reputational business impact, which refers to the damage or enhancement of the organization's image, brand, or reputation as a result of a cloud security incident. Reputational business impact can be measured by factors such as trust, loyalty, satisfaction, awareness, and perception of the organization's stakeholders, such as customers, partners, investors, regulators, and media . Option C shows how a breach reported in a timely manner to the CEO, which is a good practice for ensuring transparency and accountability in the event of a cloud security incident, can still cause reputational business impact for the customer's organization due to the public blame game between the CFO and CISO, which reflects poorly on the organization's leadership and culture and leads to the board replacing all three. Reference :=
Business Impact Analysis - Ready.gov
Business Impact Analysis - Cloud Security Alliance
What Is A Distributed Denial-of-Service (DDoS) Attack? | Cloudflare
What is Identity Theft? - Cloud Security Alliance Incident Response - Cloud Security Alliance

Question: 91

Which of the following is an example of availability technical impact?

A. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours.
B. The cloud provider reports a breach of customer personal data from an unsecured server.
C. An administrator inadvertently clicked on phish bait, exposing the company to a ransomware attack.
D. A hacker using a stolen administrator identity alters the discount percentage in the product database

Answer: A

Explanation:
An example of availability technical impact is a distributed denial of service (DDoS) attack that renders the customer's cloud inaccessible for 24 hours. Availability technical impact refers to the effect of a cloud security incident on the protection of data and services from disruption or denial. Availability is one of the three security properties of an information system, along with confidentiality and integrity.
Option A is an example of availability technical impact because it shows how a DDoS attack, which is a type of cyberattack that overwhelms a system or network with malicious traffic and prevents legitimate users from accessing it, can cause a severe and prolonged disruption of the customer's cloud services. Option A also implies that the customer's organization depends on the availability of its cloud services for its core business operations.
The other options are not examples of availability technical impact. Option B is an example of confidentiality technical impact, which refers to the effect of a cloud security incident on the protection of data from unauthorized access or disclosure. Option B shows how a breach of customer personal data from an unsecured

server, which is a type of data leakage or exposure attack that

exploits the lack of proper security controls on a system or network, can cause a violation of the privacy and security of the customer's data. Option C is an example of integrity technical impact, which refers to the effect of a cloud security incident on the protection of data from unauthorized modification or deletion. Option C shows how an administrator inadvertently clicking on phish bait, which is a type of social engineering or phishing attack that tricks a user into clicking on a malicious link or attachment, can expose the company to a ransomware attack, which is a type of malware or encryption attack that locks or encrypts the data and demands a ransom for its release. Option D is also an example of integrity technical impact, as it shows how a hacker using a stolen administrator identity, which is a type of identity theft or impersonation attack that exploits the credentials or privileges of a legitimate user to access or manipulate a system or network, can alter the discount percentage in the product database, which is a type of data tampering or corruption attack that affects the accuracy and reliability of the data. Reference :=

OWASP Risk Rating Methodology | OWASP Foundation1

OEE Factors: Availability, Performance, and Quality | OEE2

The Effects of Technological Developments on Work and Their ...

Question: 92

After finding a vulnerability in an Internet-facing server of an organization, a cybersecurity criminal is able to access an encrypted file system and successfully manages to overwrite parts of some files with random dat a. In reference to the Top Threats Analysis methodology, how would the technical impact of this incident be categorized?

A. As an integrity breach
B. As an availability breach
C. As a confidentiality breach
D. As a control breach

Answer: A

Explanation:

As an integrity breach. The technical impact of this incident can be categorized as an integrity breach, which refers to the effect of a cloud security incident on the protection of data from unauthorized modification or deletion. Integrity is one of the three security properties of an information system, along with confidentiality and availability.

The incident described in the question involves a cybersecurity criminal finding a vulnerability in an Internet-facing server of an organization, accessing an encrypted file system, and overwriting parts of some files with random data. This is a type of data tampering or corruption attack that affects the accuracy and reliability of the data. The fact that the file system was encrypted does not prevent the integrity breach, as the attacker did not need to decrypt or read the data, but only to overwrite it. The integrity breach can have serious consequences for the organization, such as data loss, data inconsistency, data recovery costs, and loss of trust.

The other options are not correct categories for the technical impact of this incident. Option B, as an availability breach, is incorrect because availability refers to the protection of data and services from disruption or denial, which is not the case in this incident. Option C, as a confidentiality breach, is incorrect because confidentiality refers to the protection of data from unauthorized access or disclosure, which is not the case in this incident. Option D, as a control breach, is incorrect because control refers to the ability to manage or influence the behavior or outcome of a system or process,

which is not a security property of an information system. Reference: =

Top Threats Analysis Methodology - CSA1
Top Threats Analysis Methodology - Cloud Security Alliance2
OWASP Risk Rating Methodology | OWASP Foundation3
OEE Factors: Availability, Performance, and Quality | OEE4
The Effects of Technological Developments on Work and Their

Question: 93

Who should define what constitutes a policy violation?

A. The external auditor
B. The organization
C. The Internet service provider (ISP)
D. The cloud provider

Answer: B

Explanation:
The organization should define what constitutes a policy violation. A policy violation refers to the breach or violation of a written policy or rule of the organization. A policy or rule is a statement that defines the expectations, standards, or requirements for the behavior, conduct, or performance of the organization's members, such as employees, customers, partners, or suppliers. Policies and rules can be based on various sources, such as laws, regulations, contracts, agreements, principles, values, ethics, or best practices12.
The organization should define what constitutes a policy violation because it is responsible for establishing, communicating, enforcing, and monitoring its own policies and rules. The organization should also define the consequences and remedies for policy violations, such as warnings, sanctions, penalties, termination, or legal action. The organization should ensure that its policies and rules are clear, consistent, fair, and aligned with its mission, vision, and goals12.
The other options are not correct. Option A, the external auditor, is incorrect because the external auditor is an independent party that provides assurance or verification of the organization's financial statements, internal controls, compliance status, or performance. The external auditor does not define the organization's policies and rules, but evaluates them against relevant standards or criteria3. Option C, the Internet service provider (ISP), is incorrect because the ISP is a company that provides access to the Internet and related services to the organization. The ISP does not define the organization's policies and rules, but may have its own policies and rules that the organization has to comply with as a customer4. Option D, the cloud provider, is incorrect because the cloud provider is a company that provides cloud computing services to the organization. The cloud provider does not define the organization's policies and rules, but may have its own policies and rules that the organization has to comply with as a customer5. Reference :=
Policy Violation Definition | Law Insider1
How to Write Policies and Procedures | Smartsheet2
What is an External Auditor? - Definition from Safeopedia3
What is an Internet Service Provider (ISP)? - Definition from Techopedia4 What is Cloud Provider? - Definition from Techopedia

Question: 94

An auditor is assessing a European organization's compliance. Which regulation is suitable if health information needs to be protected?

A. GDPR

B. DPIA

C. DPA

D. HIPAA

Answer: A

Explanation:

The General Data Protection Regulation (GDPR) is the regulation that is suitable if health information needs to be protected in the European Union. The GDPR provides the legal framework for the protection of personal data, including health data, and sets out directly applicable rules for the processing of the personal data of individuals1. The GDPR defines health data as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status2. The GDPR applies to any organization that processes health data of individuals who are in the EU, regardless of where the organization is established3.

The other options are not correct. Option B, DPIA, is incorrect because DPIA stands for Data Protection Impact Assessment, which is a process that helps organizations to identify and minimize the data protection risks of a project or activity that involves processing personal data. A DPIA is not a regulation, but a tool or a requirement under the GDPR4. Option C, DPA, is incorrect because DPA stands for Data Protection Authority, which is an independent public authority that supervises, through investigative and corrective powers, the application of the data protection law. A DPA is not a regulation, but an institution or a body under the GDPR5. Option D, HIPAA, is incorrect because HIPAA stands for Health Insurance Portability and Accountability Act, which is a US federal law that provides data privacy and security provisions for safeguarding medical information. HIPAA does not apply to the EU, but to the US6. Reference := European Health Data Space1

Article 4 - Definitions | General Data Protection Regulation (GDPR)2

Article 3 - Territorial scope | General Data Protection Regulation (GDPR)3

Data protection impact assessment | European Commission4

Data protection authorities | European Commission5 What is HIPAA? - Definition from WhatIs.com6

Question: 95

Regarding suppliers of a cloud service provider, it is MOST important for the auditor to be aware that the:

A. client organization does not need to worry about the provider's suppliers, as this is the provider's responsibility.

B. suppliers are accountable for the provider's service that they are providing.

C. client organization and provider are both responsible for the provider's suppliers.

D. client organization has a clear understanding of the provider's suppliers.

Answer: D

Explanation:

It is most important for the auditor to be aware that the client organization has a clear understanding of the provider’s suppliers. The provider’s suppliers are the third-party entities that provide services or products to the provider, such as infrastructure, software, hardware, or support. The provider’s suppliers may have a significant impact on the quality, security, reliability, and performance of the cloud services that the provider delivers to the client organization. Therefore, the auditor should ensure that the client organization knows who the provider’s suppliers are, what services or products they provide, what risks they pose, and what

contractual or regulatory obligations they have123. The other options are not correct. Option A, the client organization does not need to worry about the provider's suppliers, as this is the provider's responsibility, is incorrect because the client organization cannot rely solely on the provider to manage its suppliers. The client organization has to perform due diligence and oversight on the provider's suppliers, as they may affect the client organization's own security, compliance, and business objectives12. Option B, the suppliers are accountable for the provider's service that they are providing, is incorrect because the suppliers are not directly accountable to the client organization, but to the provider. The provider is ultimately accountable to the client organization for its service delivery and performance12. Option C, the client organization and provider are both responsible for the provider's suppliers, is incorrect because the responsibility for the provider's suppliers depends on the shared responsibility model, which defines how the security and compliance tasks and obligations are divided between the provider and the client organization. The shared responsibility model may vary depending on the type and level of cloud service that the provider offers12. Reference :=

Cloud Computing: Auditing Challenges - ISACA1

Cloud Computing: Audit Considerations - ISACA2

Top 16 Cloud Computing Companies & Service Providers 2023 - Datamation

Question: 96

Who is accountable for the use of a cloud service?

A. The cloud access security broker (CASB)
B. The supplier
C. The cloud service provider
D. The organization (client)

Answer: D

Explanation:

The organization (client) is accountable for the use of a cloud service. Accountability in cloud computing is the responsibility of cloud service providers and other parties in the cloud ecosystem to protect and properly process the data of their clients and users. However, accountability ultimately rests with the organization (client) that uses the cloud service, as it is the data owner and controller. The organization (client) has to ensure that the cloud service provider and its suppliers meet the agreed-upon service levels, security standards, and regulatory requirements. The organization

(client) also has to perform due diligence and oversight on the cloud service provider and its suppliers, as well as to comply with the shared responsibility model, which defines how the security and compliance tasks and obligations are divided between the cloud service provider and the organization (client)123.

The other options are not correct. Option A, the cloud access security broker (CASB), is incorrect because a CASB is a software tool or service that acts as an intermediary between cloud users and cloud service providers, providing visibility, data security, threat protection, and compliance. A CASB does not use the cloud service, but facilitates its secure and compliant use4. Option B, the supplier, is incorrect because a supplier is a third-party entity that provides services or products to the cloud service provider, such as infrastructure, software, hardware, or support. A supplier does not use the cloud service, but supports its delivery5. Option C, the cloud service provider, is incorrect because a cloud service provider is a company that provides cloud computing services to the organization (client). A cloud service provider does not use the cloud service, but offers it to the organization (client)6. Reference :=

Accountability Issues in Cloud Computing (5 Step ... - Medium1 Shared responsibility in the

\uE000cloud\uE001 - Microsoft Azure2 Who Is Responsible for Cloud Security? - Security Intelligence3 What is CASB? - Cloud Security Alliance4
Cloud Computing: Auditing Challenges - ISACA5
What is Cloud Provider? - Definition from Techopedia

Question: 97

Which of the following MOST enhances the internal stakeholder decision-making process for the remediation of risks identified from an organization's cloud compliance program?

A. Automating risk monitoring and reporting processes
B. Reporting emerging threats to senior stakeholders
C. Establishing ownership and accountability
D. Monitoring key risk indicators (KRIs) for multi-cloud environments

Answer: C

Explanation:
Establishing ownership and accountability most enhances the internal stakeholder decision-making process for the remediation of risks identified from an organization's cloud compliance program. Cloud compliance refers to the principle that cloud-delivered systems must comply with the standards required by their customers. Compliance requirements may include data protection regulations such as HIPAA, PCI DSS, GDPR, ISO/IEC 27001, NIST, and SOX. A cloud compliance program is a set of policies, procedures, and controls that help an organization to achieve and maintain compliance with these requirements12.
A cloud compliance program involves identifying, assessing, prioritizing, and mitigating the risks associated with using cloud services. To effectively manage these risks, an organization needs to establish ownership and accountability for each risk and its remediation. Ownership and accountability mean assigning clear roles and responsibilities to the internal stakeholders who are involved in the cloud compliance program, such as the cloud service provider, the cloud customer, the cloud users, the cloud auditors, and the cloud regulators. By doing so, an organization can ensure that the internal stakeholders have the authority, resources, and incentives to make timely and
informed decisions for the remediation of risks123.
The other options are not the most effective ways to enhance the internal stakeholder decisionmaking process for the remediation of risks. Option A, automating risk monitoring and reporting processes, is a good practice for improving the efficiency and accuracy of the cloud compliance program, but it does not address the issue of who is responsible for making decisions based on the monitoring and reporting results. Option B, reporting emerging threats to senior stakeholders, is a good practice for increasing the awareness and visibility of the cloud compliance program, but it does not address the issue of how to prioritize and respond to the emerging threats. Option D, monitoring key risk indicators (KRIs) for multi-cloud environments, is a good practice for measuring and tracking the performance and effectiveness of the cloud compliance program, but it does not address the issue of how to align and coordinate the decisions across different cloud environments123.
Reference :=
Cloud Compliance Frameworks: What You Need to Know1
Cloud Compliance: What It Is + 8 Best Practices for Improving It2
Cloud Computing: Auditing Challenges - ISACA

Question: 98

Which of the following is MOST important to manage risk from cloud vendors who might accidentally introduce unnecessary risk to an organization by adding new features to their solutions?

A. Deploying new features using cloud orchestration tools
B. Performing prior due diligence of the vendor
C. Establishing responsibility in the vendor contract
D. Implementing service level agreements (SLAs) around changes to baseline configurations

Answer: D

Explanation:

Implementing service level agreements (SLAs) around changes to baseline configurations is the most important way to manage risk from cloud vendors who might accidentally introduce unnecessary risk to an organization by adding new features to their solutions. A service level agreement (SLA) is a contract or a part of a contract that defines the expected level of service, performance, and quality that a cloud vendor will provide to an organization. An SLA can also specify the roles and responsibilities, the communication channels, the escalation procedures, and the penalties or remedies for non-compliance12.

Implementing SLAs around changes to baseline configurations can help an organization to manage the risk from cloud vendors who might add new features to their solutions without proper testing, validation, or notification. Baseline configurations are the standard or reference settings for a system or a network that are used to measure and maintain its security and performance. Changes to baseline configurations can introduce new vulnerabilities, errors, or incompatibilities that can affect the functionality, availability, or security of the system or network34. Therefore, an SLA can help an organization to ensure that the cloud vendor follows a change management process that includes steps such as risk assessment, impact analysis, approval, documentation, notification, testing, and rollback. An SLA can also help an organization to monitor and verify the changes made by the cloud vendor and to report and resolve any issues or incidents that may arise from them.

The other options are not the most effective ways to manage the risk from cloud vendors who might add new features to their solutions. Option A, deploying new features using cloud orchestration tools, is not a good way to manage the risk because cloud orchestration tools are used to automate and coordinate the deployment and management of complex cloud services and resources. Cloud orchestration tools do not address the issue of whether the new features added by the cloud vendor are necessary, secure, or compatible with the organization's system or network. Option B, performing prior due diligence of the vendor, is not a good way to manage the risk because prior due diligence is a process that involves evaluating and verifying the background, reputation, capabilities, and compliance of a potential cloud vendor before entering into a contract with them. Prior due diligence does not address the issue of how the cloud vendor will handle changes to their solutions after the contract is signed. Option C, establishing responsibility in the vendor contract, is not a good way to manage the risk because establishing responsibility in the vendor contract is a process that involves defining and assigning the roles and obligations of both parties in relation to the cloud service delivery and performance. Establishing responsibility in the vendor contract does not address the issue of how the cloud vendor will communicate and coordinate with the organization about changes to their solutions. Reference :=

What is an SLA? Best practices for service-level agreements | CIO1

Service Level Agreements - Cloud Security Alliance2

What is Baseline Configuration? - Definition from Techopedia3

Baseline Configuration - Cloud Security Alliance4

Change Management - Cloud Security Alliance Incident Response - Cloud Security Alliance What is Cloud Orchestration? - Definition from Techopedia Due Diligence - Cloud Security Alliance Contractual Security Requirements - Cloud Security Alliance

Question: 99

The BEST way to deliver continuous compliance in a cloud environment is to:

A. combine point-in-time assurance approaches with continuous monitoring.
B. increase the frequency of external audits from annual to quarterly.
C. combine point-in-time assurance approaches with continuous auditing.
D. decrease the interval between attestations of compliance

Answer: A

Explanation:
Continuous auditing is a method of auditing that provides assurance on the current state of controls and compliance in a cloud environment, rather than relying on periodic snapshots or attestations. Continuous auditing can leverage continuous monitoring data and automated tools to collect and analyze evidence of compliance, as well as alert auditors and stakeholders of any deviations or issues. Continuous auditing can complement point-in-time assurance approaches, such as certifications or audits, by providing more timely and frequent feedback on the effectiveness of controls and compliance in a cloud environment.
Reference :=
ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 821
ISACA, Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam, 2021, p. 30

Question: 100

An organization that is utilizing a community cloud is contracting an auditor to conduct a review on behalf of the group of organizations within the cloud community. Of the following, to whom should the auditor report the findings?

A. Management of the organization being audited
B. Public
C. Shareholders and interested parties
D. Cloud service provider

Answer: C

Explanation:
According to the ISACA CCAK Study Guide, the auditor should report the findings to the management of the organization being audited, as they are the primary stakeholders and decision makers for the cloud service. The management is responsible for ensuring that the cloud service meets the requirements and expectations of the community, as well as complying with any relevant laws and regulations. The auditor should also communicate the findings to the cloud service provider, as they are the secondary stakeholders and service providers for the cloud service. The cloud service provider should be aware of any issues or gaps identified by the auditor and work with the management to resolve them. The auditor should not report the findings to the public, shareholders, or interested parties, as they are not directly involved in the cloud service or its

governance. The auditor should respect the confidentiality and privacy of the community and its data, and only disclose the findings to those who have a legitimate need to know. Reference := ISACA, Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, 2021, p. 971 ISACA, Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam, 2021, p. 36

Question: 101

Which of the following standards is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an information security management system based on ISO/IEC 27001?

A. ISO/IEC 27002
B. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
C. NISTSP 800-146
D. ISO/IEC 27017:2015

Answer: D

Explanation:
ISO/IEC 27017:2015 is a standard that provides guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002, as well as additional controls with implementation guidance that specifically relate to cloud services1. ISO/IEC 27017:2015 is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an information security management system based on ISO/IEC 27001, which is the

international standard for information security management systems1. ISO/IEC 27017:2015 can help organizations to establish, implement, maintain and continually improve their information security in the cloud environment, as well as to demonstrate compliance with contractual and legal obligations1.
ISO/IEC 27002 is a code of practice for information security controls that provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems2. However, ISO/IEC 27002 does not provide specific guidance for cloud services, which is why ISO/IEC 27017:2015 was developed as an extension to ISO/IEC 27002 for cloud services1.
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a set of security controls that provides organizations with a detailed understanding of security concepts and principles that are aligned to the cloud model. The CCM is not a standard, but rather a framework that can be used to assess the overall security risk of a cloud provider. The CCM can also be mapped to other standards, such as ISO/IEC 27001 and ISO/IEC 27017:2015, to facilitate compliance and assurance activities.
NIST SP 800-146 is a publication from the National Institute of Standards and Technology (NIST) that provides an overview of cloud computing, its characteristics, service models, deployment models, benefits, challenges and considerations. NIST SP 800-146 is not a standard, but rather a reference document that can help organizations to understand the basics of cloud computing and its implications for information security. NIST SP 800-146 does not provide specific guidance or controls for cloud services, but rather refers to other standards and frameworks, such as ISO/IEC 27001 and CSA CCM, for more detailed information on cloud security. Reference :=
ISO/IEC 27017:2015 - Information technology — Security techniques ... ISO/IEC 27017:2015(en), Information technology ? Security techniques ... ISO 27017 Certification - Cloud Security Services |

NQA
An introduction to ISO/IEC 27017:2015 - 6clicks
ISO/IEC 27017:2015 - Information technology — Security techniques ...
[Cloud Controls Matrix | Cloud Security Alliance]
[NIST Cloud Computing Synopsis and Recommendations]

Question: 102

Which of the following is the BEST tool to perform cloud security control audits?

A. General Data Protection Regulation (GDPR)
B. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
C. Federal Information Processing Standard (FIPS) 140-2
D. ISO 27001

Answer: B

Explanation:
The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is the best tool to perform cloud security control audits, as it is a comprehensive framework that provides organizations with a detailed understanding of security concepts and principles that are aligned to the cloud model. The CCM covers 16 domains of cloud security, such as data security, identity and access management, encryption and key management, incident response, and audit assurance and compliance. The CCM also maps to other standards, such as ISO 27001, NIST SP 800-53, PCI DSS, COBIT, and GDPR, to facilitate compliance and assurance activities1.
The General Data Protection Regulation (GDPR) is not a tool, but rather a regulation that aims to protect the personal data and privacy of individuals in the European Union (EU) and the European Economic Area (EEA). The GDPR imposes strict requirements on organizations that process personal data of individuals in these regions, such as obtaining consent, ensuring data security, reporting breaches, and respecting data subject rights. The GDPR is relevant for cloud security audits, but it is not a comprehensive framework that covers all aspects of cloud security2.
The Federal Information Processing Standard (FIPS) 140-2 is not a tool, but rather a standard that specifies the security requirements for cryptographic modules used by federal agencies and other organizations. The FIPS 140-2 defines four levels of security, from Level 1 (lowest) to Level 4 (highest), based on the design and implementation of the cryptographic module. The FIPS 140-2 is important for cloud security audits, especially for organizations that handle sensitive or classified information, but it is not a comprehensive framework that covers all aspects of cloud security3. ISO 27001 is a standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). An ISMS is a systematic approach to managing information security risks and ensuring the confidentiality, integrity and availability of information assets. ISO 27001 is relevant for cloud security audits, as it provides a framework for assessing and improving the security posture of an organization. However, ISO 27001 does not provide specific guidance or controls for cloud services, which is why ISO 27017:2015 was developed as an extension to ISO 27001 for cloud services4. Reference := Cloud Controls Matrix | Cloud Security Alliance General Data Protection Regulation - Wikipedia FIPS PUB 140-2 - NIST
ISO/IEC 27001:2013(en), Information technology ? Security techniques ...

Question: 103

During an audit, it was identified that a critical application hosted in an off-premises cloud is not part of the organization's disaster recovery plan (DRP). Management stated that it is responsible for ensuring the cloud

service provider has a plan that is tested annually. What should be the auditor's NEXT course of action?

A. Review the contract and DR capability.
B. Plan an audit of the provider.
C. Review the security white paper of the provider.
D. Review the provider's audit reports.

Answer: A

Explanation:
The auditor's next course of action should be to review the contract and DR capability of the cloud service provider. The contract should specify the roles and responsibilities of both parties regarding disaster recovery, as well as the service level agreements (SLAs) and recovery time objectives (RTOs) for the critical application. The DR capability should demonstrate that the cloud service provider has a plan that is aligned with the organization's requirements and expectations, and that it is tested annually and validated by independent auditors. The auditor should also verify that the organization has a process to monitor and review the cloud service provider's performance and compliance with the contract and SLAs.
Planning an audit of the provider (B) may not be feasible or necessary, as the auditor may not have

access to the provider's environment or data, and may not have the authority or expertise to conduct such an audit. The auditor should rely on the provider's audit reports and certifications to assess their compliance with relevant standards and regulations.
Reviewing the security white paper of the provider © may not be sufficient or relevant, as the security white paper may not cover the specific aspects of disaster recovery for the critical application, or may not reflect the current state of the provider's security controls and practices. The security white paper may also be biased or outdated, as it is produced by the provider themselves. Reviewing the provider's audit reports (D) may be helpful, but not enough, as the audit reports may not address the specific requirements and expectations of the organization for disaster recovery, or may not cover the latest changes or incidents that may affect the provider's DR capability. The audit reports may also have limitations or qualifications that may affect their reliability or validity. Reference :=
Audit a Disaster Recovery Plan | AlertFind
ISACA Introduces New Audit Programs for Business Continuity/Disaster ...
How to Maintain and Test a Business Continuity and Disaster Recovery Plan

Question: 104

An independent contractor is assessing the security maturity of a Software as a Service (SaaS) company against industry standards. The SaaS company has developed and hosted all its products using the cloud services provided by a third-party cloud service provider. What is the optimal and most efficient mechanism to assess the controls provider is responsible for?

A. Review the provider's published questionnaires.
B. Review third-party audit reports.
C. Directly audit the provider.
D. Send a supplier questionnaire to the provider.

Answer: B

Explanation:

The optimal and most efficient mechanism to assess the controls that the provider is responsible for is to review third-party audit reports. Third-party audit reports are independent and objective assessments of the provider's security, compliance, and performance, conducted by qualified and reputable auditors. Third-party audit reports can provide assurance and evidence that the provider meets the industry standards and best practices, as well as the contractual and legal obligations with the SaaS company. Third-party audit reports can also cover a wide range of controls, such as data security, encryption, identity and access management, incident response, disaster recovery, and service level agreements. Some examples of third-party audit reports are ISO 27001 certification, SOC 1/2/3 reports, CSA STAR certification, and FedRAMP authorization123.

Reviewing the provider's published questionnaires (A) may not be optimal or efficient, as the published questionnaires may not be comprehensive or up-to-date, and may not reflect the actual state of the provider's controls. The published questionnaires may also be biased or inaccurate, as they are produced by the provider themselves.

Directly auditing the provider © may not be feasible or necessary, as the independent contractor may not have access to the provider's environment or data, and may not have the authority or expertise to conduct such an audit. The independent contractor should rely on the third-party audit reports and certifications to assess the provider's compliance with relevant standards and regulations.

Sending a supplier questionnaire to the provider (D) may not be optimal or efficient, as the supplier questionnaire may not cover all the aspects of the provider's controls, and may not provide sufficient evidence or assurance of the provider's security maturity. The supplier questionnaire may also take a long time to complete and verify, and may not be consistent with the industry standards and best practices. Reference :=

How to Evaluate Cloud Service Provider Security (Checklist)

Cloud service review process - Cloud Adoption Framework

How to choose a cloud service provider | Microsoft Azure

Question: 105

In all three cloud deployment models, (IaaS, PaaS, and SaaS), who is responsible for the patching of the hypervisor layer?

A. Cloud service provider

B. Shared responsibility

C. Cloud service customer

D. Patching on hypervisor layer not required

Answer: A

Explanation:

The cloud service provider is responsible for the patching of the hypervisor layer in all three cloud deployment models (IaaS, PaaS, and SaaS). The hypervisor layer is the software that allows the creation and management of virtual machines on a physical server. The hypervisor layer is part of the cloud infrastructure, which is owned and operated by the cloud service provider. The cloud service provider is responsible for ensuring that the hypervisor layer is secure, reliable, and up to date with the latest patches and updates. The cloud service provider should also monitor and report on the status and performance of the hypervisor layer, as well as any

issues or incidents that may affect it. The cloud service customer is not responsible for the patching of the hypervisor layer, as they do not have access or control over the cloud infrastructure. The cloud service customer only has access and control over the cloud resources and services that they consume from the cloud service provider, such as virtual machines, storage, databases, applications, etc. The cloud service customer is responsible for ensuring that their own cloud resources and services are secure, compliant, and updated with the latest patches and updates.

The patching of the hypervisor layer is not a shared responsibility between the cloud service provider and the cloud service customer, as it is solely under the domain of the cloud service provider. The shared responsibility model in cloud computing refers to the division of security and compliance responsibilities between the cloud service provider and the cloud service customer, depending on the type of cloud deployment model. For example, in IaaS, the cloud service provider is responsible for securing the physical infrastructure, network, and hypervisor layer, while the cloud service customer is responsible for securing their own operating systems, applications, data, etc. In PaaS, the cloud service provider is responsible for securing everything up to the platform layer, while the cloud service customer is responsible for securing their own applications and data. In SaaS, the cloud service provider is responsible for securing everything up to the application layer, while the cloud service customer is responsible for securing their own data and user access.

Patching on hypervisor layer is required, as it is essential for maintaining the security, reliability, and performance of the cloud infrastructure. Patching on hypervisor layer can help prevent vulnerabilities, bugs, errors, or exploits that may compromise or affect the functionality of the virtual machines or other cloud resources and services. Patching on hypervisor layer can also help improve or enhance the features or capabilities of the hypervisor software or hardware. Reference := Patching process - AWS Prescriptive Guidance

What is a Hypervisor in Cloud Computing and Its Types? - Simplilearn

In all three cloud deployment models, (IaaS, PaaS, and ... - Exam4Training

Reference Architecture: App Layering | Citrix Tech Zone

Hypervisor - GeeksforGeeks

Question: 106

To ensure a cloud service provider is complying with an organization's privacy requirements, a cloud auditor should FIRST review:

A. organizational policies, standards, and procedures.
B. adherence to organization policies, standards, and procedures.
C. legal and regulatory requirements.
D. the IT infrastructure.

Answer: A

Explanation:

To ensure a cloud service provider is complying with an organization's privacy requirements, a cloud auditor should first review the organizational policies, standards, and procedures that define the privacy objectives, expectations, and responsibilities of the organization. The organizational policies, standards, and procedures should also reflect the legal and regulatory requirements that apply to the organization and its cloud service provider, as well as the best practices and guidelines for cloud privacy. The organizational policies, standards, and procedures should provide the basis for evaluating the cloud service provider's privacy practices and controls, as well as the contractual terms and conditions that govern the cloud service agreement. The cloud auditor should compare the organizational policies, standards, and procedures with the cloud service

provider's selfdisclosure statements, third-party audit reports, certifications, attestations, or other evidence of compliance123.

Reviewing the adherence to organization policies, standards, and procedures (B) is a subsequent step that the cloud auditor should perform after reviewing the organizational policies, standards, and procedures themselves. The cloud auditor should assess whether the cloud service provider is following the organization's policies, standards, and procedures consistently and effectively, as well as whether the organization is monitoring and enforcing the compliance of the cloud service provider. The cloud auditor should also identify any gaps or deviations between the organization's policies, standards, and procedures and the actual practices and controls of the cloud service provider123.

Reviewing the legal and regulatory requirements © is an important aspect of ensuring a cloud service provider is complying with an organization's privacy requirements, but it is not the first step that a cloud auditor should take. The legal and regulatory requirements may vary depending on the jurisdiction, industry, or sector of the organization and its cloud service provider. The legal and regulatory requirements may also change over time or be subject to interpretation or dispute. Therefore, the cloud auditor should first review the organizational policies, standards, and procedures that incorporate and translate the legal and regulatory requirements into specific and measurable privacy objectives, expectations, and responsibilities for both parties123.

Reviewing the IT infrastructure (D) is not a relevant or sufficient step for ensuring a cloud service provider is complying with an organization's privacy requirements. The IT infrastructure refers to the hardware, software, network, and other components that support the delivery of cloud services. The IT infrastructure is only one aspect of cloud security and privacy, and it may not be accessible or visible to the cloud auditor or the organization. The cloud auditor should focus on reviewing the privacy practices and controls that are implemented by the cloud service provider at different layers of the cloud service model (IaaS, PaaS, SaaS), as well as the contractual terms and conditions that define the privacy rights and obligations of both parties123. Reference :=

Cloud Audits and Compliance: What You Need To Know - Linford & Company LLP

Trust in the Cloud in audits of cloud services - PwC

Cloud Compliance & Regulations Resources | Google Cloud

Question: 107

The effect of which of the following should have priority in planning the scope and objectives of a cloud audit?

A. Applicable industry good practices
B. Applicable statutory requirements
C. Organizational policies and procedures
D. Applicable corporate standards

Answer: B

Explanation:

The effect of applicable statutory requirements should have priority in planning the scope and objectives of a cloud audit, as they are the mandatory and enforceable rules that govern the cloud service provider and the cloud service customer. Statutory requirements may vary depending on the jurisdiction, industry, or sector of the cloud service provider and the cloud service customer, as well as the type, location, and sensitivity of the data processed or stored in the cloud. Statutory requirements may include laws, regulations, standards, or codes that relate to data protection, privacy, security, compliance, governance, taxation, or liability. The cloud auditor should identify and understand the applicable statutory requirements that affect the cloud service

provider and the cloud service customer, and assess whether they are met and adhered to by both parties. The cloud auditor should also verify that the contractual terms and conditions between the cloud service provider and the cloud service customer reflect and comply with the applicable statutory requirements123.

Applicable industry good practices (A) are important for planning the scope and objectives of a cloud audit, but they are not as high priority as applicable statutory requirements. Industry good practices are the recommended or accepted methods or techniques for achieving a desired outcome or result in a specific domain or context. Industry good practices may include frameworks, guidelines, principles, or best practices that are developed by professional bodies, associations, or organizations that have expertise or authority in a certain field or area. Industry good practices may help the cloud service provider and the cloud service customer to improve their performance, quality, efficiency, or effectiveness in delivering or using cloud services. However, industry good practices are not mandatory or enforceable, and they may vary or change over time depending on the evolution of technology or business needs123.

Organizational policies and procedures © are important for planning the scope and objectives of a cloud audit, but they are not as high priority as applicable statutory requirements. Organizational policies and procedures are the internal rules and guidelines that define the objectives, expectations, and responsibilities of an organization regarding its operations, activities, processes, or functions. Organizational policies and procedures may include mission statements, vision statements, values statements, strategies, goals, plans, standards, manuals, handbooks, or instructions that are specific to an organization. Organizational policies and procedures may help the organization to align its actions and decisions with its purpose and direction, as well as to ensure consistency and accountability among its members or stakeholders. However, organizational policies and procedures are not mandatory or enforceable outside the organization, and they may differ or conflict among different organizations123.

Applicable corporate standards (D) are important for planning the scope and objectives of a cloud audit, but they are not as high priority as applicable statutory requirements. Corporate standards are the internal rules and guidelines that define the minimum level of quality, performance, reliability, or compatibility that an organization expects from its products, services, processes, or systems. Corporate standards may include specifications, criteria, metrics, indicators, benchmarks, or baselines that are specific to an organization. Corporate standards may help the organization to measure and evaluate its outputs or outcomes against its objectives or expectations, as well as to identify and address any gaps or issues that may arise. However, corporate standards are not mandatory or enforceable outside the organization, and they may differ or conflict among different organizations123. Reference :=

Cloud Audits: A Guide for Cloud Service Providers - Cloud Standards ...

Cloud Audits: A Guide for Cloud Service Customers - Cloud Standards ... Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam

Question: 108

Which of the following is the MOST significant difference between a cloud risk management program and a traditional risk management program?

A. Virtualization of the IT landscape
B. Shared responsibility model
C. Risk management practices adopted by the cloud service provider
D. Hosting sensitive information in the cloud environment

Answer: B

Explanation:

The most significant difference between a cloud risk management program and a traditional risk management program is the shared responsibility model. The shared responsibility model is the division of security and compliance responsibilities between the cloud service provider and the cloud service customer, depending on the type of cloud service model (IaaS, PaaS, SaaS). The shared responsibility model implies that both parties have to collaborate and coordinate to ensure that the cloud service meets the required level of security and compliance, as well as to identify and mitigate any risks that may arise from the cloud environment123.

Virtualization of the IT landscape (A) is a difference between a cloud risk management program and a traditional risk management program, but it is not the most significant one. Virtualization of the IT landscape refers to the abstraction of physical IT resources, such as servers, storage, network, or applications, into virtual ones that can be accessed and managed over the internet. Virtualization of the IT landscape enables the cloud service provider to offer scalable, flexible, and efficient cloud services to the cloud service customer. However, virtualization of the IT landscape also introduces new risks, such as data leakage, unauthorized access, misconfiguration, or performance degradation123.

Risk management practices adopted by the cloud service provider © are a difference between a cloud risk management program and a traditional risk management program, but they are not the most significant one. Risk management practices adopted by the cloud service provider refer to the methods or techniques that the cloud service provider uses to identify, assess, treat, monitor, and report on the risks that affect their cloud services. Risk management practices adopted by the cloud service provider may include policies, standards, procedures, controls, audits, certifications, or attestations that demonstrate their security and compliance posture. However, risk management practices adopted by the cloud service provider are not sufficient or reliable on their own, as they may not cover all aspects of cloud security and compliance, or may not align with the expectations or requirements of the cloud service customer123.

Hosting sensitive information in the cloud environment (D) is a difference between a cloud risk management program and a traditional risk management program, but it is not the most significant one. Hosting sensitive information in the cloud environment refers to storing or processing data that are confidential, personal, or valuable in the cloud infrastructure or platform that is owned and operated by the cloud service provider. Hosting sensitive information in the cloud environment can offer benefits such as cost savings, accessibility, availability, or backup. However, hosting sensitive information in the cloud environment also poses risks such as data breaches, privacy violations, compliance failures, or legal disputes123. Reference :=

Cloud Risk Management - ISACA

Cloud Risk Management: A Primer for Security Professionals - Infosec ...

Cloud Risk Management: A Primer for Security Professionals - Infosec ...

Question: 109

In audit parlance, what is meant by "management representation"?

A. A person or group of persons representing executive management during audits
B. A mechanism to represent organizational structure
C. A project management technique to demonstrate management's involvement in key project stages
D. Statements made by management in response to specific inquiries

Answer: D

Explanation:

Management representation is a term used in audit parlance to refer to the statements made by management in response to specific inquiries or through the financial statements, as part of the audit evidence that the auditor obtains. Management representation can be oral or written, but the auditor usually obtains written representation from management in the form of a letter that attests to the accuracy and completeness of the financial statements and other information provided to the auditor. The management representation letter is signed by senior management, such as the CEO and CFO, and is dated the same date of audit work completion. The management representation

letter confirms or documents the representations explicitly or implicitly given to the auditor during the audit, indicates the continuing appropriateness of such representations, and reduces the possibility of misunderstanding concerning the matters that are the subject of the representations12. Management representation is not a person or group of persons representing executive management during audits (A), as this would imply that management is not directly involved or accountable for the audit process. Management representation is not a mechanism to represent organizational structure (B), as this would imply that management representation is a graphical or diagrammatic tool to show the hierarchy or relationships within an organization. Management representation is not a project management technique to demonstrate management's involvement in key project stages ©, as this would imply that management representation is a method or practice to monitor or report on the progress or outcomes of a project.

Question: 110

Which of the following is a good candidate for continuous auditing?

A. Procedures
B. Governance
C. Cryptography and authentication
D. Documentation quality

Answer: C

Explanation:

Cryptography and authentication are good candidates for continuous auditing, as they are critical aspects of cloud security that require constant monitoring and verification. Cryptography and authentication refer to the methods and techniques that ensure the confidentiality, integrity, and availability of data and communications in the cloud environment. Cryptography involves the use of encryption algorithms and keys to protect data from unauthorized access or modification. Authentication involves the use of credentials and tokens to verify the identity and access rights of users or devices. Continuous auditing can help to assess the effectiveness and compliance of cryptography and authentication controls, such as data encryption, key management, password policies, multifactor authentication, single sign-on, etc. Continuous auditing can also help to detect and alert any anomalies or issues that may compromise or affect cryptography and authentication, such as data breaches, key leakage, password cracking, unauthorized access, etc123.

Procedures (A) are not good candidates for continuous auditing, as they are not specific or measurable aspects of cloud security that can be easily automated or tested. Procedures refer to the steps or actions that are performed to achieve a certain objective or result in a specific domain or context. Procedures may vary depending on the type, nature, or complexity of the task or process involved. Continuous auditing requires a clear and consistent definition of the expected outcome or output, as well as the criteria or metrics to evaluate

it. Procedures may not provide such a definition or criteria, and may require human judgment or interpretation to assess their effectiveness or compliance123.

Governance (B) is not a good candidate for continuous auditing, as it is not a specific or measurable aspect of cloud security that can be easily automated or tested. Governance refers to the framework or system that defines the roles, responsibilities, policies, standards, procedures, and practices for managing and overseeing an organization or a domain. Governance may involve multiple stakeholders, such as management, board of directors, regulators, auditors, customers, etc., who

have different interests, expectations, or perspectives. Continuous auditing requires a clear and consistent definition of the expected outcome or output, as well as the criteria or metrics to evaluate it. Governance may not provide such a definition or criteria, and may require human judgment or interpretation to assess its effectiveness or compliance123.

Documentation quality (D) is not a good candidate for continuous auditing, as it is not a specific or measurable aspect of cloud security that can be easily automated or tested. Documentation quality refers to the degree to which the documents that describe or support an organization or a domain are accurate, complete, consistent, relevant, and understandable. Documentation quality may depend on various factors, such as the purpose, audience, format, style, language, structure, content, etc., of the documents involved. Continuous auditing requires a clear and consistent definition of the expected outcome or output, as well as the criteria or metrics to evaluate it. Documentation quality may not provide such a definition or criteria, and may require human judgment or interpretation to assess its effectiveness or compliance123. Reference :=

Cloud Audits: A Guide for Cloud Service Providers - Cloud Standards ...

Cloud Audits: A Guide for Cloud Service Customers - Cloud Standards ... Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam

Question: 111

What areas should be reviewed when auditing a public cloud?

A. Patching and configuration
B. Vulnerability management and cyber security reviews
C. Identity and access management (IAM) and data protection
D. Source code reviews and hypervisor

Answer: C

Explanation:

Identity and access management (IAM) and data protection are the areas that should be reviewed when auditing a public cloud, as they are the key aspects of cloud security and compliance that affect both the cloud service provider and the cloud service customer. IAM and data protection refer to the methods and techniques that ensure the confidentiality, integrity, and availability of data and resources in the cloud environment. IAM involves the use of credentials, policies, roles, permissions, and tokens to verify the identity and access rights of users or devices. Data protection involves the use of encryption, backup, recovery, deletion, and retention to protect data from unauthorized access, modification, loss, or disclosure123.

Patching and configuration (A) are not the areas that should be reviewed when auditing a public cloud, as they are not the key aspects of cloud security and compliance that affect both the cloud service provider and the cloud service customer. Patching and configuration refer to the processes and practices that ensure the security, reliability, and performance of the cloud infrastructure, platform, or software. Patching involves the use of updates or fixes to address vulnerabilities, bugs, errors, or exploits that may compromise or affect the

functionality of the cloud components. Configuration involves the use of settings or parameters to customize or optimize the functionality of the cloud components. Patching and configuration are mainly under the responsibility of the cloud service provider, as they own and operate the cloud infrastructure, platform, or software. The cloud service customer has limited or no access or control over these aspects123. Vulnerability management and cyber security reviews (B) are not the areas that should be reviewed when auditing a public cloud, as they are not specific or measurable aspects of cloud security and compliance that can be easily audited or tested. Vulnerability management and cyber security reviews refer to the processes and practices that identify, assess, treat, monitor, and report on the risks that affect the security posture of an organization or a domain. Vulnerability management involves the use of tools or techniques to scan, analyze, prioritize, remediate, or mitigate vulnerabilities that may expose an organization or a domain to threats or attacks. Cyber security reviews involve the use of tools or techniques to evaluate, measure, benchmark, or improve the security capabilities or maturity of an organization or a domain. Vulnerability management and cyber security reviews are general or broad terms that encompass various aspects of cloud security and compliance, such as IAM, data protection, patching, configuration, etc. Therefore, they are not specific or measurable areas that can be audited or tested individually123. Source code reviews and hypervisor (D) are not the areas that should be reviewed when auditing a public cloud, as they are not relevant or accessible aspects of cloud security and compliance for most cloud service customers. Source code reviews refer to the processes and practices that examine the source code of software applications or systems to identify errors, bugs, vulnerabilities, or inefficiencies that may affect their quality, functionality, or security. Hypervisor refers to the software that allows the creation and management of virtual machines on a physical server. Source code reviews and hypervisor are mainly under the responsibility of the cloud service provider, as they own and operate the software applications or systems that deliver cloud services. The cloud service customer has no access or control over these aspects123. Reference := Cloud Audits: A Guide for Cloud Service Providers - Cloud Standards ... Cloud Audits: A Guide for Cloud Service Customers - Cloud Standards ... Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam

Question: 112

What aspect of Software as a Service (SaaS) functionality and operations would the cloud customer be responsible for and should be audited?

A. Source code reviews
B. Patching
C. Access controls
D. Vulnerability management

Answer: C

Explanation:

Access controls are the aspect of Software as a Service (SaaS) functionality and operations that the cloud customer is responsible for and should be audited. Access controls refer to the methods and techniques that verify the identity and access rights of users or devices that access or use the SaaS application and its data. Access controls may include credentials, policies, roles, permissions, tokens, multifactor authentication, single sign-on, etc. The cloud customer is responsible for ensuring that only authorized and legitimate users or devices can access or use the SaaS application and its data, as well as for protecting the confidentiality, integrity, and availability of their data. The cloud customer should also monitor and audit the access and usage of the SaaS application and its data, as well as any incidents or issues that may affect them123.

Source code reviews (A) are not the aspect of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Source code reviews refer to the processes and practices that examine the source code of software applications or systems to identify errors, bugs, vulnerabilities, or inefficiencies that may affect their quality, functionality, or security. Source code reviews are mainly under the responsibility of the cloud service provider, as they own and operate the software applications or systems that deliver SaaS services. The cloud customer has no access or control over these aspects123.

Patching (B) is not the aspect of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Patching refers to the processes and practices that ensure the security, reliability, and performance of the cloud infrastructure, platform, or software. Patching involves the use of updates or fixes to address vulnerabilities, bugs, errors, or exploits that may compromise or affect the functionality of the cloud components. Patching is mainly under the responsibility of the cloud service provider, as they own and operate the cloud infrastructure, platform, or software. The cloud customer has limited or no access or control over these aspects123. Vulnerability management (D) is not the aspect of SaaS functionality and operations that the cloud customer is responsible for and should be audited. Vulnerability management refers to the processes and practices that identify, assess, treat, monitor, and report on the risks that affect the security posture of an organization or a domain. Vulnerability management involves the use of tools or techniques to scan, analyze, prioritize, remediate, or mitigate vulnerabilities that may expose an organization or a domain to threats or attacks. Vulnerability management is mainly under the responsibility of the cloud service provider, as they own and operate the cloud infrastructure, platform, or software. The cloud customer has limited or no access or control over these aspects123. Reference :=

Cloud Audits: A Guide for Cloud Service Providers - Cloud Standards ...

Cloud Audits: A Guide for Cloud Service Customers - Cloud Standards ... Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam

Question: 113

Which of the following would be the MOST critical finding of an application security and DevOps audit?

A. Certifications with global security standards specific to cloud are not reviewed, and the impact of noted findings are not assessed.

B. Outsourced cloud service interruption, breach, or loss of stored data occurred at the cloud service provider.

C. The organization is not using a unified framework to integrate cloud compliance with regulatory requirements.

D. Application architecture and configurations did not consider security measures.

Answer: D

Explanation:

The most critical finding of an application security and DevOps audit would be that the application architecture and configurations did not consider security measures. This finding would indicate that the application is vulnerable to various threats and attacks, such as data breaches, unauthorized access, injection, cross-site scripting, denial-of-service, etc. This finding would also imply that the application does not comply with the security standards and best practices for cloud services, such as ISO/IEC 27017:20151, CSA Cloud Controls Matrix2, or NIST SP 800-1463. This finding would require immediate remediation and improvement of the application security posture, as well as the

implementation of security controls and tests throughout the DevOps process.
Certifications with global security standards specific to cloud are not reviewed, and the impact of noted findings are not assessed (A) would be a significant finding of an application security and DevOps audit, but not the most critical one. This finding would indicate that the organization is not aware or informed of the security requirements and expectations for cloud services, as well as the gaps or issues that may affect their compliance or performance. This finding would require regular review and analysis of the certifications with global security standards specific to cloud, such as ISO/IEC 270014, CSA STAR Certification, or FedRAMP Authorization, as well as the assessment of the impact of noted findings on the organization's risk profile and business objectives.
Outsourced cloud service interruption, breach, or loss of stored data occurred at the cloud service provider (B) would be a serious finding of an application security and DevOps audit, but not the most critical one. This finding would indicate that the cloud service provider failed to ensure the availability, confidentiality, and integrity of the cloud services and data that they provide to the organization. This finding would require investigation and resolution of the root cause and impact of the incident, as well as the implementation of preventive and corrective measures to avoid recurrence. This finding would also require review and verification of the contractual terms and conditions between the organization and the cloud service provider, as well as the service level agreements (SLAs) and recovery time objectives (RTOs) for the cloud services.
The organization is not using a unified framework to integrate cloud compliance with regulatory requirements © would be an important finding of an application security and DevOps audit, but not the most critical one. This finding would indicate that the organization is not following a consistent and systematic approach to manage and monitor its cloud compliance with regulatory requirements, such as GDPR, HIPAA, PCI DSS, etc. This finding would require adoption and implementation of a unified framework to integrate cloud compliance with regulatory requirements, such as COBIT, NIST Cybersecurity Framework, or CIS Controls, as well as the alignment and integration of these frameworks with the DevOps process.

Question: 114

Which of the following aspects of risk management involves identifying the potential reputational and financial harm when an incident occurs?

A. Likelihood
B. Mitigation
C. Residual risk
D. Impact analysis

Answer: D

Explanation:
Impact analysis is the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Impact analysis is the process of estimating the consequences or effects of a risk event on the business objectives, operations, processes, or functions. Impact analysis helps to measure and quantify the severity or magnitude of the risk event, as well as to prioritize and rank the risks based on their impact. Impact analysis also helps to determine the appropriate level of response and mitigation for each risk event, as well as to allocate the necessary resources and budget for risk management123.
Likelihood (A) is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Likelihood is the aspect of risk management that involves estimating the probability or frequency of a risk event occurring. Likelihood is the process of assessing and evaluating the factors or causes that may trigger or influence a risk event, such as threats, vulnerabilities,

assumptions, uncertainties, etc. Likelihood helps to measure and quantify the chance or possibility of a risk event happening, as well as to prioritize and rank the risks based on their likelihood123.

Mitigation (B) is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Mitigation is the aspect of risk management that involves reducing or minimizing the likelihood or impact of a risk event. Mitigation is the process of implementing and applying controls or actions that can prevent, avoid, transfer, or accept a risk event, depending on the risk appetite and tolerance of the organization. Mitigation helps to improve and enhance the security and resilience of the organization against potential risks, as well as to optimize the cost and benefit of risk management123.

Residual risk © is not the aspect of risk management that involves identifying the potential reputational and financial harm when an incident occurs. Residual risk is the aspect of risk management that involves measuring and monitoring the remaining or leftover risk after mitigation. Residual risk is the process of evaluating and reviewing the effectiveness and efficiency of the mitigation controls or actions, as well as identifying and addressing any gaps or issues that may arise. Residual risk helps to ensure that the actual level of risk is aligned with the desired level of risk, as well as to update and improve the risk management strategy and plan123.

Reference := Risk Analysis: A Comprehensive Guide | SafetyCulture
Risk Assessment and Analysis Methods: Qualitative and Quantitative - ISACA Risk Management Process - Risk Management | Risk Assessment | Risk ...

Question: 115

Which of the following is the FIRST step of the Cloud Risk Evaluation Framework?

A. Analyzing potential impact and likelihood
B. Establishing cloud risk profile
C. Evaluating and documenting the risks
D. Identifying key risk categories

Answer: D

Explanation:

The first step of the Cloud Risk Evaluation Framework is to identify key risk categories. Key risk categories are the broad areas or domains of cloud security and compliance that may affect the cloud service provider and the cloud service customer. Key risk categories may include data security, identity and access management, encryption and key management, incident response, disaster recovery, audit assurance and compliance, etc. Identifying key risk categories helps to scope and focus the cloud risk assessment process, as well as to prioritize and rank the risks based on their relevance and significance. Identifying key risk categories also helps to align and map the risks with the applicable standards, regulations, or frameworks that govern cloud security and compliance12. Analyzing potential impact and likelihood (A) is not the first step of the Cloud Risk Evaluation Framework, but rather the third step. Analyzing potential impact and likelihood is the process of estimating the consequences or effects of a risk event on the business objectives, operations, processes, or functions (impact), as well as the probability or frequency of a risk event occurring (likelihood). Analyzing potential impact and likelihood helps to measure and quantify the severity or magnitude of the risk event, as well as to prioritize and rank the risks based on their impact and likelihood12.

Establishing cloud risk profile (B) is not the first step of the Cloud Risk Evaluation Framework, but rather the second step. Establishing cloud risk profile is the process of defining and documenting the expected level of risk

that an organization is willing to accept or tolerate in relation to its cloud services (risk appetite), as well as the actual level of risk that an organization faces or encounters in relation to its cloud services (risk exposure). Establishing cloud risk profile helps to determine and communicate the objectives, expectations, and responsibilities of cloud security and compliance, as well as to align and integrate them with the business strategy and goals12.

Evaluating and documenting the risks © is not the first step of the Cloud Risk Evaluation Framework, but rather the fourth step. Evaluating and documenting the risks is the process of assessing and reporting on the effectiveness and efficiency of the controls or actions that are implemented or applied to prevent, avoid, transfer, or accept a risk event (risk treatment), as well as identifying and addressing any gaps or issues that may arise (risk monitoring). Evaluating and documenting the risks helps to ensure that the actual level of risk is aligned with the desired level of risk, as well as to update and improve the risk management strategy and plan12. Reference := Cloud Auditing Knowledge: Preparing for the CCAK Certificate Exam

Cloud Risk—10 Principles and a Framework for Assessment - ISACA

Question: 116

When performing audits in relation to business continuity management and operational resilience strategy, what would be the MOST critical aspect to audit in relation to the strategy of the cloud customer that should be formulated jointly with the cloud service provider?

A. Validate whether the strategy covers all aspects of business continuity and resilience planning, taking inputs from the assessed impact and risks, to consider activities for before, during, and after a disruption.

B. Validate whether the strategy is developed by both cloud service providers and cloud service consumers within the acceptable limits of their risk appetite.

C. Validate whether the strategy covers all activities required to continue and recover prioritized activities within identified time frames and agreed capacity, aligned to the risk appetite of the organization including the invocation of continuity plans and crisis management capabilities.

Answer: A

Explanation:

Question: 117

DevSecOps aims to integrate security tools and processes directly into the software development life cycle and should be done:

A. at the end of the development cycle.

B. after go-live.

C. in all development steps.

D. at the beginning of the development cycle.

Answer: C

Explanation:

According to the CCAK Study Guide, the business continuity management and operational resilience strategy of the cloud customer should be formulated jointly with the cloud service provider, as they share the responsibility for ensuring the availability and recoverability of the cloud services. The strategy should cover all aspects of business continuity and resilience planning, taking inputs from the assessed impact and risks, to consider activities for before, during, and after a disruption. These activities include prevention, mitigation, response, recovery, restoration, and improvement. The strategy should also define the roles and responsibilities of both parties, the communication channels and escalation procedures, the testing and exercising plans, and the review and update mechanisms1

The other options are not correct because:

Option B is not correct because the strategy should not only be developed within the acceptable limits of the risk appetite, but also aligned with the business objectives and stakeholder expectations of both parties. The risk appetite is only one of the factors that influence the strategy formulation1 Option C is not correct because the strategy should not only cover the activities required to continue and recover prioritized activities within identified time frames and agreed capacity, but also consider the activities for before and after a disruption, such as prevention, mitigation, improvement, etc. The strategy should also include other elements such as roles and responsibilities, communication channels, testing plans, etc1

Reference: 1: ISACA, Cloud Security Alliance. Certificate of Cloud Auditing Knowledge (CCAK) Study Guide. 2021. pp. 83-84.

Question: 118

What is a sign that an organization has adopted a shift-left concept of code release cycles?

A. Large entities with slower release cadences and geographically dispersed systems
B. Incorporation of automation to identify and address software code problems early
C. A waterfall model remove resources through the development to release phases
D. Maturity of start-up entities with high-iteration to low-volume code commits

Answer: B

Explanation:

The shift-left concept of code release cycles is a practice that aims to integrate testing, quality, and performance evaluation early in the software development life cycle, often before any code is written. This helps to find and prevent defects, improve quality, and enable faster delivery of secure software. One of the key aspects of the shift-left concept is the incorporation of automation to identify and address software code problems early, such as using continuous integration, continuous delivery, and continuous testing tools. Automation can help reduce manual errors, speed up feedback loops, and increase efficiency and reliability123

The other options are not correct because:

Option A is not correct because large entities with slower release cadences and geographically dispersed systems are more likely to face challenges in adopting the shift-left concept, as they may have more complex and legacy systems, dependencies, and processes that hinder agility and collaboration. The shift-left concept requires a culture of continuous improvement, experimentation, and learning that may not be compatible with traditional or siloed organizations4 Option C is not correct because a waterfall model is the opposite of the shift-left concept, as it involves sequential phases of development, testing, and deployment that are performed late in the software development life cycle. A waterfall model does not allow for early detection and correction of defects, feedback, or changes, and can result in higher costs, delays, and risks5

Option D is not correct because maturity of start-up entities with high-iteration to low-volume code commits is not a sign of the shift-left concept, but rather a sign of the agile or lean software development methodologies. These methodologies focus on delivering value to customers by delivering working software in short iterations or sprints, with frequent feedback and adaptation. While these methodologies can support the shift-left concept by enabling faster testing and delivery cycles, they are not equivalent or synonymous with it6 Reference: 1: AWS. What is DevSecOps? - Developer Security Operations Explained - AWS. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 2: Dynatrace. Shift left vs shift right: A DevOps mystery solved - Dynatrace news. [Online]. Available: 2. [Accessed: 14-Apr-2023]. 3: BMC Software. Shift Left Testing: What, Why & How To Shift Left – BMC Software | Blogs. [Online]. Available: 3. [Accessed: 14-Apr-2023]. 4: GitLab. How to shift left with continuous integration | GitLab. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 5: DZone. DevOps and The ShiftLeft Principle - DZone. [Online]. Available: 5. [Accessed: 14-Apr-2023]. 6: Devopedia. Shift Left - Devopedia. [Online]. Available: 6. [Accessed: 14-Apr-2023].

Question: 119

The MOST important goal of regression testing is to ensure:

A. the expected outputs are provided by the new features.
B. the system can handle a high number of users.
C. the system can be restored after a technical issue.
D. new releases do not impact previous stable features.

Answer: D

Explanation:

According to the definition of regression testing, it is a type of software testing that confirms that a recent program or code change has not adversely affected existing features1 It involves re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change2 If the software does not perform as expected, it is called a regression. Therefore, the most important goal of regression testing is to ensure new releases do not impact previous stable features.

The other options are not correct because:

Option A is not correct because the expected outputs are provided by the new features is not the goal of regression testing, but rather the goal of functional testing or acceptance testing. These types of testing aim to verify that the software meets the specified requirements and satisfies the user needs. Regression testing, on the other hand, focuses on checking that the existing features are not broken by the new features3

Option B is not correct because the system can handle a high number of users is not the goal of regression testing, but rather the goal of performance testing or load testing. These types of testing aim to evaluate the behavior and responsiveness of the software under various workloads and conditions. Regression testing, on the other hand, focuses on checking that the software functionality and quality are not degraded by code changes4

Option C is not correct because the system can be restored after a technical issue is not the goal of regression testing, but rather the goal of recovery testing or disaster recovery testing. These types of testing aim to assess the ability of the software to recover from failures or disasters and resume normal operations. Regression testing, on the other hand, focuses on checking that the software does not introduce new failures or defects due to code changes5

Reference: 1: Wikipedia. Regression testing - Wikipedia. [Online]. Available: 3. [Accessed: 14-Apr- 2023]. 2:

Katalon. What is Regression Testing? Definition, Tools, Examples - Katalon. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 3: Guru99. What is Functional Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 4: Guru99. What is Performance Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 5: Guru99. What is Recovery Testing? with Example - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023].

Question: 120

To ensure integration of security testing is implemented on large code sets in environments where time to completion is critical, what form of validation should an auditor expect?

A. Parallel testing
B. Full application stack unit testing
C. Functional verification
D. Regression testing

Answer: D

Explanation:

Regression testing is a type of software testing that confirms that a recent program or code change has not adversely affected existing features1 It involves re-running functional and non-functional tests to ensure that previously developed and tested software still performs as expected after a change2 Regression testing is suitable for large code sets in environments where time to completion is critical, as it can help detect and prevent defects, improve quality, and enable faster delivery of secure software. Regression testing can be automated to reduce manual errors, speed up feedback loops, and increase efficiency and reliability3

The other options are not correct because:

Option A is not correct because parallel testing is a type of software testing that involves testing multiple applications or subsystems concurrently to reduce the test time4 Parallel testing does not necessarily ensure the integration of security testing, as it depends on the quality and coverage of the test cases and scenarios used for each application or subsystem. Parallel testing may also introduce challenges such as synchronization, coordination, and communication among the testers and developers5

Option B is not correct because full application stack unit testing is a type of software testing that involves testing individual units or components of an application in isolation to verify their functionality, logic, interfaces, and performance6 Full application stack unit testing does not ensure the integration of security testing, as it does not consider the interactions and dependencies among the units or components, or the behavior of the application as a whole. Unit testing is typically performed by developers at an early stage of the software development life cycle, and may not cover all the security aspects or requirements of the application7

Option C is not correct because functional verification is a type of software testing that involves verifying that the software meets the specified requirements and satisfies the user needs. Functional verification does not ensure the integration of security testing, as it does not focus on how the software is designed or configured, or how it handles malicious or unexpected inputs. Functional verification is typically performed by quality assurance teams at a later stage of the software development life cycle, and may not detect all the security vulnerabilities or risks of the software. Reference: 1: Wikipedia. Regression testing - Wikipedia. [Online]. Available: 3. [Accessed: 14-Apr- 2023]. 2: Katalon. What is Regression Testing? Definition, Tools, Examples - Katalon. [Online]. Available: 4. [Accessed: 14-Apr-2023]. 3: BMC Software. Shift Left Testing: What, Why & How To Shift Left – BMC Software | Blogs. [Online]. Available: 3. [Accessed: 14-Apr-2023]. 4: Guru99. What is Parallel Testing? with Example - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 5: LambdaTest. Parallel Testing

In Selenium WebDriver | LambdaTest Blog. [Online]. Available: . [Accessed: 14-Apr-2023]. 6: Guru99. What is Unit Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. 7: Software Testing Help. Unit Testing Vs Integration Testing: Difference Between These Two - SoftwareTestingHelp.com Blog. [Online]. Available: . [Accessed: 14- Apr-2023]. : Guru99. What is Functional Testing? Types & Examples - Guru99. [Online]. Available: . [Accessed: 14-Apr-2023]. : Software Testing Help. Functional Testing Vs Non-Functional Testing - SoftwareTestingHelp.com Blog. [Online]. Available: . [Accessed: 14-Apr-2023].

Question: 121

Which of the following BEST ensures adequate restriction on the number of people who can access the pipeline production environment?

A. Ensuring segregation of duties in the production and development pipelines
B. Periodic review of the continuous integration and continuous delivery (CI/CD) pipeline audit logs to identify any access violations
C. Role-based access controls in the production and development pipelines
D. Separation of production and development pipelines

Answer: C

Explanation:

Role-based access control (RBAC) is a method of restricting access to resources based on the roles of individual users within an organization1 RBAC can help ensure adequate restriction on the number of people who can access the pipeline production environment, as it can limit the permissions and actions that each user can perform on the pipeline resources, such as code, secrets, environments, etc. RBAC can also help enforce the principle of least privilege, which states that users should only have the minimum level of access required to perform their tasks2

The other options are not correct because:

Option A is not correct because ensuring segregation of duties in the production and development pipelines is not sufficient to ensure adequate restriction on the number of people who can access the pipeline production environment. Segregation of duties is a practice that aims to prevent fraud, errors, or conflicts of interest by dividing responsibilities among different people or teams3 However, segregation of duties does not necessarily limit the number of people who can access the pipeline resources, as it depends on how the roles and permissions are defined and assigned. Segregation of duties is also more relevant for preventing unauthorized changes or deployments to the production environment, rather than restricting access to it4

Option B is not correct because periodic review of the continuous integration and continuous delivery (CI/CD) pipeline audit logs to identify any access violations is not a proactive measure to ensure adequate restriction on the number of people who can access the pipeline production environment. Audit logs are records of events or activities that occur within a system or process5 Audit logs can help monitor and detect any unauthorized or suspicious access to the pipeline resources, but they cannot prevent or restrict such access in the first place. Audit logs are also dependent on the frequency and quality of the review process, which may not be timely or effective enough to mitigate the risks of access violations6

Option D is not correct because separation of production and development pipelines is not a direct way to ensure adequate restriction on the number of people who can access the pipeline production environment. Separation of production and development pipelines is a practice that aims to isolate and protect the production environment from any potential errors, bugs, or vulnerabilities that may arise from the

development process. However, separation of pipelines does not automatically imply restriction of access, as it depends on how the roles and permissions are configured for each pipeline. Separation of pipelines may also introduce challenges such as synchronization, coordination, and communication among the pipeline teams and stakeholders.

Reference: 1: Wikipedia. Role-based access control - Wikipedia. [Online]. Available: 1. [Accessed: 14- Apr-2023]. 2: Microsoft Learn. Set pipeline permissions - Azure Pipelines | Microsoft Learn. [Online]. Available: 1. [Accessed: 14-Apr-2023]. 3: Investopedia. Segregation Of Duties Definition - Investopedia.com Blog. [Online]. Available: . [Accessed: 14-Apr-2023]. 4: Cider Security. Insufficient PBAC (Pipeline-Based Access Controls) - Cider Security Blog. [Online]. Available: . [Accessed: 14-Apr- 2023]. 5: Wikipedia. Audit trail - Wikipedia. [Online]. Available: . [Accessed: 14-Apr-2023]. 6: Microsoft Learn. Securing Azure Pipelines - Azure Pipelines | Microsoft Learn. [Online]. Available: . [Accessed: 14-Apr-2023]. : AWS DevOps Blog. How to implement CI/CD with AWS CodePipeline - AWS DevOps Blog | Amazon Web Services Blog. [Online]. Available: . [Accessed: 14-Apr-2023]. : LambdaTest. What Is Parallel Testing? with Example - LambdaTest Blog. [Online]. Available: . [Accessed: 14-Apr-2023].

Question: 122

An auditor identifies that a cloud service provider received multiple customer inquiries and requests for proposal (RFPs) during the last month.

Which of the following should be the BEST recommendation to reduce the provider's burden?

A. The provider can schedule a call with each customer.
B. The provider can share all security reports with customers to streamline the process.
C. The provider can answer each customer individually.
D. The provider can direct all customer inquiries to the information in the CSA STAR registry

Answer: D

Explanation:

The CSA STAR registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings1 The registry is designed for users of cloud services to assess their cloud providers' security and compliance posture, including the regulations, standards, and frameworks they adhere to1 The registry also promotes industry transparency and reduces complexity and costs for both providers and customers2

The provider can direct all customer inquiries to the information in the CSA STAR registry, as this would be the best recommendation to reduce the provider's burden. By publishing to the registry, the provider can show current and potential customers their security and compliance posture, without having to fill out multiple customer questionnaires or requests for proposal (RFPs)2 The provider can also leverage the different levels of assurance available in the registry, such as selfassessment, third-party audit, or certification, to demonstrate their security maturity and trustworthiness1 The provider can also benefit from the CSA Trusted Cloud Providers program, which recognizes providers that have fulfilled additional training and volunteer requirements with CSA, demonstrating their commitment to cloud security competency and industry best practices3 The other options are not correct because:

Option A is not correct because the provider can schedule a call with each customer is not a good recommendation to reduce the provider's burden. Scheduling a call with each customer would be time-consuming, inefficient, and impractical, especially if the provider receives multiple inquiries and RFPs every month. Scheduling a call would also not guarantee that the customer would be satisfied with the provider's security and compliance posture, as they may still request additional information or evidence. Scheduling a call would also not help the provider differentiate themselves from other providers in the market, as they may not

be able to showcase their security maturity and trustworthiness effectively.

Option B is not correct because the provider can share all security reports with customers to streamline the process is not a good recommendation to reduce the provider's burden. Sharing all security reports with customers may not be feasible, as some reports may contain sensitive or confidential information that should not be disclosed to external parties. Sharing all security reports may also not be desirable, as some reports may be outdated, incomplete, or inconsistent, which could undermine the provider's credibility and reputation. Sharing all security reports may also not be effective, as some customers may not have the expertise or resources to review and understand them properly.

Option C is not correct because the provider can answer each customer individually is not a good recommendation to reduce the provider's burden. Answering each customer individually would be tedious, repetitive, and costly, as the provider would have to provide similar or identical information to different customers over and over again. Answering each customer individually would also not ensure that the provider's security and compliance posture is consistent and accurate, as they may make mistakes or omissions in their responses. Answering each customer individually would also not help the provider stand out from other providers in the market, as they may not be able to highlight their security achievements and certifications.

Reference: 1: STAR | CSA 2: Why your cloud services need the CSA STAR Registry listing 3: STAR Registry | CSA

Question: 123

The PRIMARY purpose of Open Certification Framework (OCF) for the CSA STAR program is to:

A. facilitate an effective relationship between the cloud service provider and cloud client.
B. ensure understanding of true risk and perceived risk by the cloud service users.
C. provide global, accredited, and trusted certification of the cloud service provider.
D. enable the cloud service provider to prioritize resources to meet its own requirements.

Answer: C

Explanation:

According to the CSA website, the primary purpose of the Open Certification Framework (OCF) for the CSA STAR program is to provide global, accredited, trusted certification of cloud providers1 The OCF is an industry initiative to allow global, trusted independent evaluation of cloud providers. It is a program for flexible, incremental and multi-layered cloud provider certification and/or attestation according to the Cloud Security Alliance's industry leading security guidance and control framework2 The OCF aims to address the gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services, such as the lack of simple, cost effective ways to evaluate and compare providers' resilience, data protection, privacy, and service portability2 The OCF also aims to promote industry transparency and reduce complexity and costs for both providers and customers3

The other options are not correct because:

Option A is not correct because facilitating an effective relationship between the cloud service provider and cloud client is not the primary purpose of the OCF for the CSA STAR program, but rather a potential benefit or outcome of it. The OCF can help facilitate an effective relationship between the provider and the client by providing a common language and framework for assessing and communicating the security and compliance posture of the provider, as well as enabling trust and confidence in the provider's capabilities and performance. However, this is not the main goal or objective of the OCF, but rather a means to achieve it.

Option B is not correct because ensuring understanding of true risk and perceived risk by the cloud service

users is not the primary purpose of the OCF for the CSA STAR program, but rather a possible implication or consequence of it. The OCF can help ensure understanding of true risk and perceived risk by the cloud service users by providing objective and verifiable information and evidence about the provider's security and compliance level, as well as allowing comparison and benchmarking with other providers in the market. However, this is not the main aim or intention of the OCF, but rather a result or effect of it.

Option D is not correct because enabling the cloud service provider to prioritize resources to meet its own requirements is not the primary purpose of the OCF for the CSA STAR program, but rather a potential advantage or opportunity for it. The OCF can enable the cloud service provider to prioritize resources to meet its own requirements by providing a flexible, incremental and multi-layered approach to certification and/or attestation that allows the provider to choose the level of assurance that suits their business needs and goals. However, this is not the main reason or motivation for the OCF, but rather a benefit or option for it.

Reference: 1: Open Certification Framework Working Group | CSA 2: Open Certification Framework | CSA - Cloud Security Alliance 3: Why your cloud services need the CSA STAR Registry listing

Question: 124

Which of the following is the MOST important audit scope document when conducting a review of a cloud service provider?

A. Processes and systems to be audited
B. Updated audit work program
C. Documentation criteria for the audit evidence
D. Testing procedure to be performed

Answer: A

Explanation:

According to the definition of audit scope, it is the extent and boundaries of an audit, which include the audit objectives, the activities and documents covered, the time period and locations audited, and the related activities not audited1 Audit scope determines how deeply an audit is performed and may vary depending on the type of audit. Audit scope can also mean the examination of a person or the inspection of the books, records, or accounts of a person for tax purposes1 The most important audit scope document when conducting a review of a cloud service provider is the processes and systems to be audited. This document defines the specific areas and aspects of the cloud service provider that will be subject to the audit, such as the cloud service delivery model, the cloud deployment model, the cloud security domains, the cloud service level agreements, the cloud governance framework, etc2 The processes and systems to be audited document also helps to identify the risks, controls, criteria, and objectives of the audit, as well as the roles and responsibilities of the auditors and the auditees3 The processes and systems to be audited document is essential for planning and performing an effective and efficient audit of a cloud service provider. The other options are not correct because:

Option B is not correct because the updated audit work program is not an audit scope document, but rather an audit planning document. The audit work program is a set of detailed instructions or procedures that guide the auditor in conducting the audit activities4 The audit work program is based on the audit scope, but it does not define it. The audit work program may also change during the course of the audit, depending on the findings and issues encountered by the auditor4 Option C is not correct because the documentation criteria for the audit evidence is not an audit scope document, but rather an audit quality document. The documentation criteria for the audit evidence is a set of standards or guidelines that specify what constitutes sufficient and appropriate evidence to support the auditor's conclusions and opinions5 The documentation criteria for the audit evidence is derived from the audit scope, but it does not determine it. The documentation criteria for the

audit evidence may also vary depending on the nature and source of the evidence collected by the auditor5

Option D is not correct because the testing procedure to be performed is not an audit scope document, but rather an audit execution document. The testing procedure to be performed is a set of steps or actions that describe how to test or verify a specific control or process within the cloud service provider6 The testing procedure to be performed is aligned with the audit scope, but it does not establish it. The testing procedure to be performed may also differ depending on the type and level of testing required by the auditor6

Reference: 1: AUDIT SCOPE DEFINITION - VentureLine 2: Audit Scope and Criteria - Auditor Training Online 3: Open Certification Framework | CSA - Cloud Security Alliance 4: Audit Work Program Definition - Audit Work Program Example 5: INTERNATIONAL STANDARD ON AUDITING 230 AUDIT DOCUMENTATION CONTENTS - IFAC 6: What are Testing Procedures? - Definition from Techopedia

Question: 125

A certification target helps in the formation of a continuous certification framework by incorporating:

A. the service level objective (SLO) and service qualitative objective (SQO).
B. the scope description and security attributes to be tested.
C. the frequency of evaluating security attributes.
D. CSA STAR level 2 attestation.

Answer: B

Explanation:

According to the blog article "Continuous Auditing and Continuous Certification" by the Cloud Security Alliance, a certification target helps in the formation of a continuous certification framework by incorporating the scope description and security attributes to be tested1 A certification target is a set of security objectives that a cloud service provider (CSP) defines and commits to fulfill as part of the continuous certification process1 Each security objective is associated with a policy that specifies the assessment frequency, such as every four hours, every day, or every week1 A certification target also includes a set of tools that are capable of verifying that the security objectives are met, such as automated scripts, APIs, or third-party services1

The other options are not correct because:

Option A is not correct because the service level objective (SLO) and service qualitative objective (SQO) are not part of the certification target, but rather part of the service level agreement (SLA) between the CSP and the cloud customer. An SLO is a measurable characteristic of the cloud service, such as availability, performance, or reliability. An SQO is a qualitative characteristic of the cloud service, such as security, privacy, or compliance2 The SLA defines the expected level of service and the consequences of not meeting it. The SLA may be used as an input for defining the certification target, but it is not equivalent or synonymous with it.

Option C is not correct because the frequency of evaluating security attributes is not the only component of the certification target, but rather one aspect of it. The frequency of evaluating security attributes is determined by the policy that is associated with each security objective in the certification target. The policy defines how often the security objective should be verified by the tools, such as every four hours, every day, or every week1 However, the frequency alone does not define the certification target, as it also depends on the scope description and the security attributes to be tested.

Option D is not correct because CSA STAR level 2 attestation is not a component of the certification target, but rather a prerequisite for it. CSA STAR level 2 attestation is a third-party independent assessment of the CSP's security posture based on ISO/IEC 27001 and CSA Cloud Controls Matrix (CCM)3 CSA STAR level 2 attestation provides a baseline assurance level for the CSP before they can define and implement their certification target for continuous certification. CSA STAR level 2 attestation is also required for CSA STAR level 3 certification, which is based on continuous auditing and continuous certification3

Reference: 1: Continuous Auditing and Continuous Certification - Cloud Security Alliance 2: Service Level

Agreement | CSA 3: Open Certification Framework | CSA - Cloud Security Alliance

Question: 126

Why should the results of third-party audits and certification be relied on when analyzing and assessing the cybersecurity risks in the cloud?

A. To establish an audit mindset within the organization
B. To contrast the risk generated by the loss of control
C. To reinforce the role of the internal audit function
D. To establish an accountability culture within the organization

Answer: B

Explanation:
One possible reason why the results of third-party audits and certification should be relied on when analyzing and assessing the cybersecurity risks in the cloud is to contrast the risk generated by the loss of control. When an organization moves its data and processes to the cloud, it inevitably loses some degree of control over its security and compliance posture, as it depends on the cloud service provider (CSP) to implement and maintain adequate security measures and controls1 This loss of control can increase the organization's exposure to various cybersecurity risks, such as data breaches, unauthorized access, denial of service, malware infection, etc2
To mitigate these risks, the organization needs to have a clear understanding of the security and compliance level of the CSP, as well as the shared responsibility model that defines the roles and responsibilities of both parties3 Third-party audits and certification can provide some level of assurance that the CSP meets certain standards and requirements related to security and compliance, such as ISO/IEC 27001, CSA STAR, SOC 2, etc. These audits and certification can also help the organization compare and contrast the security posture of different CSPs in the market, as well as identify any gaps or weaknesses that need to be addressed or compensated.
Therefore, relying on the results of third-party audits and certification can help the organization contrast the risk generated by the loss of control in the cloud, and make informed decisions about selecting and managing its cloud services.
Reference: 1: Security in the Cloud: Are Audits and Certifications Really Enough?3 2: Understanding The Third-Party Impact On Cybersecurity Risk - Forbes2 3: Open Certification Framework | CSA - Cloud Security Alliance : Reducing Cybersecurity Security Risk From and to Third Parties - ISACA1 : Why your cloud services need the CSA STAR Registry listing

Question: 127

If a customer management interface is compromised over the public Internet, it can lead to:

A. incomplete wiping of the data.
B. computing and data compromise for customers.
C. ease of acquisition of cloud services.
D. access to the RAM of neighboring cloud computers.

Answer: B

Explanation:

Customer management interfaces are the web portals or applications that allow customers to access and manage their cloud services, such as provisioning, monitoring, billing, etc. These interfaces are exposed to the public Internet and may be vulnerable to attacks such as phishing, malware, denial- of-service, or credential theft. If an attacker compromises a customer management interface, they can potentially access and manipulate the customer's cloud resources, data, and configurations, leading to computing and data compromise for customers. This can result in data breaches, service disruptions, unauthorized transactions, or other malicious activities.

Reference:

Cloud Computing - Security Benefits and Risks | PPT - SlideShare1, slide 10

Cloud Security Risks: The Top 8 According To ENISA - CloudTweaks2, section on Management Interface Compromise

Certificate of Cloud Auditing Knowledge (CCAK) Study Guide, section 2.3.2.1 : https://www.isaca.org/-/media/info/ccak/ccak-study-guide.pdf

Question: 128

Which of the following is a detective control that may be identified in a Software as a Service (SaaS) service provider?

A. Data encryption
B. Incident management
C. Network segmentation
D. Privileged access monitoring

Answer: D

Explanation:

A detective control is a type of internal control that seeks to uncover problems in a company's processes once they have occurred1. Examples of detective controls include physical inventory checks, reviews of account reports and reconciliations, as well as assessments of current controls1. Detective controls use platform telemetry to detect misconfigurations, vulnerabilities, and potentially malicious activity in the cloud environment2.

In a Software as a Service (SaaS) service provider, privileged access monitoring is a detective control that can help identify unauthorized or suspicious activities by users who have elevated permissions to access or modify cloud resources, data, or configurations. Privileged access monitoring can involve logging, auditing, alerting, and reporting on the actions performed by privileged users3. This can help detect security incidents, compliance violations, or operational errors in a timely manner and enable appropriate responses.

Data encryption, incident management, and network segmentation are examples of preventive controls, which are designed to prevent problems from occurring in the first place. Data encryption protects the confidentiality and integrity of data by transforming it into an unreadable format that can only be decrypted with a valid key1. Incident management is a process that aims to restore normal service operations as quickly as possible after a disruption or an adverse event4. Network segmentation divides a network into smaller subnetworks that have different access levels and security policies, reducing the attack surface and limiting the impact of a breach1.

Reference:

Detective controls - SaaS Lens - docs.aws.amazon.com3, section on Privileged access monitoring Detective

controls | Cloud Architecture Center | Google Cloud2, section on Detective controls Internal control: how do preventive and detective controls work?4, section on SaaS Solutions to Support Internal Control Detective Control: Definition, Examples, Vs. Preventive Control1, section on What Is a Detective Control?

Question: 129

Which of the following is an example of a corrective control?

A. A central antivirus system installing the latest signature files before allowing a connection to the network
B. All new employees having standard access rights until their manager approves privileged rights
C. Unsuccessful access attempts being automatically logged for investigation
D. Privileged access to critical information systems requiring a second factor of authentication using a soft token

Answer: C

Explanation:
A corrective control is a measure taken to correct or reduce the impact of an error, deviation, or unwanted activity1. Corrective control can be either manual or automated, depending on the type of control used. Corrective control can involve procedures, manuals, systems, patches, quarantines, terminations, reboots, or default dates1. A Business Continuity Plan (BCP) is an example of a corrective control.
Unsuccessful access attempts being automatically logged for investigation is an example of a corrective control because it is a response to a potential security incident that aims to identify and resolve the cause and prevent future occurrences2. Logging and investigating failed login attempts can help detect unauthorized or malicious attempts to access sensitive data or systems and take appropriate actions to mitigate the risk.
The other options are examples of preventive controls, which are designed to prevent problems from occurring in the first place3. Preventive controls can include:
A central antivirus system installing the latest signature files before allowing a connection to the network: This is a preventive control because it prevents malware infection by blocking potentially harmful connections and updating the antivirus software regularly4.
All new employees having standard access rights until their manager approves privileged rights: This is a preventive control because it prevents unauthorized access by enforcing the principle of least privilege and requiring approval for granting higher-level permissions5.
Privileged access to critical information systems requiring a second factor of authentication using a soft token: This is a preventive control because it prevents credential theft or compromise by adding an extra layer of security to verify the identity of the user.
Reference:
What is a corrective control? - Answers1, section on Corrective control
Detective controls - SaaS Lens - docs.aws.amazon.com2, section on Unsuccessful login attempts Internal control: how do preventive and detective controls work?3, section on Preventive Controls What Are Security Controls? - F54, section on Preventive Controls
The 3 Types of Internal Controls (With Examples) | Layer Blog5, section on Preventive Controls
What are the 3 Types of Internal Controls? — RiskOptics - Reciprocity, section on Preventive Controls

Question: 130

When mapping controls to architectural implementations, requirements define:

A. control objectives.
B. control activities.
C. guidelines.
D. policies.

Answer: B

Explanation:
Requirements define control activities, which are the actions, processes, or mechanisms that are implemented to achieve the control objectives1. Control objectives are the targets or desired conditions to be met that are designed to ensure that policy intent is met2. Guidelines are the recommended practices or advice that provide flexibility in how to implement a policy, standard, or control3. Policies are the statements of management's intent that establish the direction, purpose, and scope of an organization's internal control system4.

Reference:
COSO – Control Activities - Deloitte1, section on Control Activities
Words Matter - Understanding Policies, Control Objectives, Standards ...2, section on Control Objectives
Understanding Policies, Control Objectives, Standards, Guidelines ...3, section on Guidelines Internal Control Handbook4, section on Policies

Question: 131

During the cloud service provider evaluation process, which of the following BEST helps identify baseline configuration requirements?

A. Vendor requirements
B. Product benchmarks
C. Benchmark controls lists
D. Contract terms and conditions

Answer: C

Explanation:
: During the cloud service provider evaluation process, benchmark controls lists BEST help identify baseline configuration requirements. Benchmark controls lists are standardized sets of security and compliance controls that are applicable to different cloud service models, deployment models, and industry sectors1. They provide a common framework and language for assessing and comparing the security posture and capabilities of cloud service providers2. They also help cloud customers to define their own security and compliance requirements and expectations based on best practices and industry standards3.
Some examples of benchmark controls lists are:
The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), which is a comprehensive list of 133 control objectives that cover 16 domains of cloud security4.
The National Institute of Standards and Technology (NIST) Special Publication 800-53, which is a catalog of 325 security and privacy controls for federal information systems and organizations, including cloud-based systems5.
The International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27017, which is a code of practice that provides guidance on 121 information security controls for cloud services based on ISO/IEC 270026.
Vendor requirements, product benchmarks, and contract terms and conditions are not the best sources for

identifying baseline configuration requirements. Vendor requirements are the specifications and expectations that the cloud service provider has for its customers, such as minimum hardware, software, network, or support requirements7. Product benchmarks are the measurements and comparisons of the performance, quality, or features of different cloud services or products8. Contract terms and conditions are the legal agreements that define the rights, obligations, and responsibilities of the parties involved in a cloud service contract9. These sources may provide some information on the configuration requirements, but they are not as comprehensive, standardized, or objective as benchmark controls lists.

Reference:

CSA Security Guidance for Cloud Computing | CSA1, section on Identify necessary security and compliance requirements

Evaluation Criteria for Cloud Infrastructure as a Service - Gartner2, section on Security Controls Checklist: Cloud Services Provider Evaluation Criteria | Synoptek3, section on Security Cloud Controls Matrix | CSA4, section on Overview

NIST Special Publication 800-53 - NIST Pages5, section on Abstract

ISO/IEC 27017:2015(en), Information technology — Security techniques …6, section on Scope What is vendor management? Definition from WhatIs.com7, section on Vendor management What is Benchmarking? Definition from WhatIs.com8, section on Benchmarking

What is Terms and Conditions? Definition from WhatIs.com9, section on Terms and Conditions

Question: 132

What is the MOST effective way to ensure a vendor is compliant with the agreed-upon cloud service?

A. Examine the cloud provider's certifications and ensure the scope is appropriate.
B. Document the requirements and responsibilities within the customer contract
C. Interview the cloud security team and ensure compliance.
D. Pen test the cloud service provider to ensure compliance.

Answer: A

Explanation:

The most effective way to ensure a vendor is compliant with the agreed-upon cloud service is to examine the cloud provider's certifications and ensure the scope is appropriate. Certifications are independent attestations of the cloud provider's compliance with various standards, regulations, and best practices related to cloud security, privacy, and governance1. They provide assurance to customers that the cloud provider has implemented adequate controls and processes to meet their contractual obligations and expectations2. However, not all certifications are equally relevant or comprehensive, so customers need to verify that the certifications cover the specific cloud service, region, and data type that they are using3. Customers should also review the certification reports or audit evidence to understand the scope, methodology, and results of the assessment4.

The other options are not as effective as examining the cloud provider's certifications. Documenting the requirements and responsibilities within the customer contract is an important step to establish the terms and conditions of the cloud service agreement, but it does not guarantee that the vendor will comply with them5. Customers need to monitor and verify the vendor's performance and compliance on an ongoing basis. Interviewing the cloud security team may provide some insights into the vendor's compliance practices, but it may not be sufficient or reliable without independent verification or documentation. Pen testing the cloud service provider may reveal some vulnerabilities or weaknesses in the vendor's security posture, but it may not cover all aspects of compliance or be authorized by the vendor. Pen testing should be done with caution and

consent, as it may cause disruption or damage to the cloud service or violate the terms of service.

Reference:

Cloud Compliance: What You Need To Know - Linford & Company LLP1, section on Cloud Compliance

Cloud Services Due Diligence Checklist | Trust Center2, section on Why Microsoft created the Cloud Services Due Diligence Checklist

The top cloud providers for government | ZDNET3, section on What is FedRAMP?

Cloud Computing Security Considerations | Cyber.gov.au4, section on Certification

Cloud Audits and Compliance: What You Need To Know - Linford & Company LLP5, section on Cloud Compliance Management

Cloud Services Due Diligence Checklist | Trust Center, section on How to use the checklist

Cloud Computing Security Considerations | Cyber.gov.au, section on Security governance

The top cloud providers for government | ZDNET, section on Penetration testing

Penetration Testing in AWS - Amazon Web Services (AWS), section on Introduction

Question: 133

Which of the following is MOST useful for an auditor to review when seeking visibility into the cloud supply chain for a newly acquired Software as a Service (SaaS) solution?

A. SaaS provider contract
B. Payments made by the service owner
C. SaaS vendor white papers
D. Cloud compliance obligations register

Answer: A

Explanation:

The most useful document for an auditor to review when seeking visibility into the cloud supply chain for a newly acquired Software as a Service (SaaS) solution is the SaaS provider contract. The contract is the legal agreement that defines the terms and conditions of the cloud service, including the roles, responsibilities, and obligations of the parties involved1. The contract should also specify the service level agreements (SLAs), security and privacy requirements, data ownership and governance, incident response and reporting, audit rights and access, and subcontracting or outsourcing arrangements of the SaaS provider2. By reviewing the contract, the auditor can gain insight into the cloud supply chain and assess the risks, controls, and compliance of the SaaS solution.

The other options are not as useful as the SaaS provider contract. Payments made by the service owner are the financial transactions that reflect the fees or charges incurred by using the SaaS solution. They may indicate the usage or consumption of the cloud service, but they do not provide much information about the cloud supply chain or its security and compliance aspects3. SaaS vendor white papers are the marketing or educational materials that describe the features, benefits, or best practices of the SaaS solution. They may provide some general or technical information about the cloud service, but they are not legally binding or verifiable4. Cloud compliance obligations register is a tool that helps customers identify and track their compliance requirements and obligations for using cloud services. It may help customers understand their own responsibilities and risks in relation to the cloud service, but it does not necessarily reflect the compliance status or performance of the SaaS provider5.

Reference:

Cloud Services Due Diligence Checklist | Trust Center1, section on How to use the checklist

Cloud Computing Security Considerations | Cyber.gov.au2, section on Contractual arrangements

Cloud Computing Pricing Models: A Comparison - DZone Cloud3, section on Pricing Models
What is a White Paper? Definition from WhatIs.com4, section on White Paper
Cloud Compliance Obligations Register | Cyber.gov.au5, section on Cloud Compliance Obligations Register

Question: 134

Which of the following is the PRIMARY area for an auditor to examine in order to understand the criticality of the cloud services in an organization, along with their dependencies and risks?

A. Contractual documents of the cloud service provider
B. Heat maps
C. Data security process flow
D. Turtle diagram

Answer: B

Explanation:
Heat maps are graphical representations of data that use color-coding to show the relative intensity, frequency, or magnitude of a variable1. Heat maps can be used to visualize the criticality of the cloud services in an organization, along with their dependencies and risks, by mapping the cloud services to different dimensions, such as business impact, availability, security, performance, cost, etc. Heat maps can help auditors identify the most important or vulnerable cloud services, as well as the relationships and trade-offs among them2.
For example, Azure Charts provides heat maps for various aspects of Azure cloud services, such as updates, trends, pillars, areas, geos, categories, etc3. These heat maps can help auditors understand the current state and dynamics of Azure cloud services and compare them across different dimensions4.
Contractual documents of the cloud service provider are the legal agreements that define the terms and conditions of the cloud service, including the roles, responsibilities, and obligations of the parties involved. They may provide some information on the criticality of the cloud services in an organization, but they are not as visual or comprehensive as heat maps. Data security process flow is a diagram that shows the steps and activities involved in protecting data from unauthorized access, use, modification, or disclosure. It may help auditors understand the data security controls and risks of the cloud services in an organization, but it does not cover other aspects of criticality, such as business impact or performance. Turtle diagram is a tool that helps analyze a process by showing its inputs, outputs, resources, criteria, methods, and interactions. It may help auditors understand the process flow and dependencies of the cloud services in an organization, but it does not show the relative importance or risks of each process element.
Reference:
What is a Heat Map? Definition from WhatIs.com1, section on Heat Map
Cloud Computing Security Considerations | Cyber.gov.au2, section on Cloud service criticality
Azure Charts - Clarity for the Cloud3, section on Heat Maps
Azure Services Overview4, section on Heat Maps
Cloud Services Due Diligence Checklist | Trust Center, section on How to use the checklist Data Security Process Flow - an overview | ScienceDirect Topics, section on Data Security Process Flow
What is a Turtle Diagram? Definition from WhatIs.com, section on Turtle Diagram

Question: 135

Which of the following would be the GREATEST governance challenge to an organization where production

is hosted in a public cloud and backups are held on the premises?

A. Aligning the cloud service delivery with the organization's objectives
B. Aligning shared responsibilities between provider and customer
C. Aligning the cloud provider's service level agreement (SLA) with the organization's policy
D. Aligning the organization's activity with the cloud provider's policy

Answer: B

Explanation:
The greatest governance challenge in the scenario where production is hosted in a public cloud and backups are held on-premises is aligning the shared responsibilities between the provider and the customer. This is because the division of security and compliance duties must be clearly understood and managed to ensure that all aspects of the cloud services are adequately protected and meet regulatory requirements. The customer is responsible for the security 'in' the cloud (i.e., the data and applications), while the provider is responsible for the security 'of' the cloud (i.e., the infrastructure). Misalignment in this shared responsibility model can lead to gaps in security and compliance, making it a significant governance challenge.
Reference = This answer is verified by the information available in the Cloud Auditing Knowledge (CCAK) documents and related resources provided by ISACA and the Cloud Security Alliance (CSA), which discuss the shared responsibility model and its implications for governance in cloud environments12.

Question: 136

Which of the following is the BEST method to demonstrate assurance in the cloud services to multiple cloud customers?

A. Provider's financial stability report and market value
B. Reputation of the service provider in the industry
C. Provider self-assessment and technical documents
D. External attestation and certification audit reports

Answer: D

Explanation:
External attestation and certification audit reports are considered the best method to demonstrate assurance in cloud services to multiple customers because they provide an independent verification of the cloud service provider's controls and practices. These reports are conducted by third-party auditors and offer a level of transparency and trust that cannot be achieved through self-assessments or internal documents. They help ensure that the cloud provider meets industry standards and regulatory requirements, which is crucial for customers to assess the risk and compliance posture of

their cloud service providers.
Reference = The importance of external attestation and certification audit reports is supported by the Cloud Security Alliance (CSA) and ISACA, which state that the CCAK credential prepares IT and security professionals to ensure that the right controls are in place and to mitigate the risks and costs of audit management and penalties for non-compliance1.

Question: 137

Which of the following activities are part of the implementation phase of a cloud assurance program during a cloud migration?

A. Development of the monitoring goals and requirements
B. Identification of processes, functions, and systems
C. Identification of roles and responsibilities
D. Identification of the relevant laws, regulations, and standards

Answer: A

Explanation:
During the implementation phase of a cloud assurance program, the focus is on establishing the operational aspects that will ensure the ongoing security and compliance of the cloud environment. This includes developing the monitoring goals and requirements which are essential for setting up the assurance framework. It involves determining what needs to be monitored, how it should be monitored, and the metrics that will be used to measure compliance and performance.
Reference = The information aligns with best practices for cloud migration and assurance programs as outlined in various resources, including the Cloud Assurance Program Guide by Microsoft Cybersecurity1, which discusses the importance of developing and implementing policies for cloud data and system migration, and the Enterprise Guide to Successful Cloud Adoption by New Relic2, which emphasizes the role of observability in cloud migration, including the establishment of monitoring goals.

Question: 138

Which of the following would be considered as a factor to trust in a cloud service provider?

A. The level of willingness to cooperate
B. The level of exposure for public information
C. The level of open source evidence available
D. The level of proven technical skills

Answer: C

Explanation:
Trust in a cloud service provider is fundamentally based on the assurance that the provider can deliver secure and reliable services. The level of proven technical skills is a critical factor because it demonstrates the provider's capability to implement and maintain robust security measures, manage complex cloud infrastructures, and respond effectively to technical challenges. Technical

expertise is essential for establishing trust, as it directly impacts the security and performance of the cloud services offered.
Reference = The importance of technical skills in establishing trust is supported by the resources provided by ISACA and the Cloud Security Alliance (CSA). These resources emphasize the need for cloud service providers to have a strong technical foundation to ensure the fulfillment of internal requirements, proper controls, and compliance with regulations, which are crucial for maintaining customer trust and mitigating risks1234.

Question: 139

What is the FIRST thing to define when an organization is moving to the cloud?

A. Goals of the migration
B. Internal service level agreements (SLAs)
C. Specific requirements
D. Provider evaluation criteria

Answer: A

Explanation:
When an organization is moving to the cloud, the first thing to define is the goals of the migration. This is because the goals will guide all subsequent decisions and strategies. Defining clear goals helps in understanding what the organization wants to achieve with cloud migration, whether it's cost savings, scalability, improved performance, or something else. These goals are essential for aligning the migration with the business objectives and for setting the direction for the cloud strategy. Reference = The importance of defining the goals of cloud migration is supported by the resources provided by the Cloud Security Alliance (CSA) and ISACA in their Cloud Auditing Knowledge (CCAK) materials12. These resources emphasize the need for a clear understanding of the objectives and benefits expected from moving to the cloud, which is foundational before delving into specifics such as SLAs, requirements, or provider evaluation criteria.

Question: 140

To BEST prevent a data breach from happening, cryptographic keys should be:

A. distributed in public-facing repositories.
B. embedded in source code.
C. rotated regularly.
D. transmitted in clear text.

Answer: C

Explanation:
Rotating cryptographic keys regularly is a security best practice that helps to mitigate the risk of unauthorized access to encrypted data. When keys are rotated, old keys are retired and replaced with new ones, making any compromised keys useless to an attacker. This process helps to limit the time window during which a stolen key can be used to breach data. Key rotation is a fundamental

aspect of key management lifecycle best practices, which include generating new key pairs, rotating keys at set intervals, revoking access to keys, and destroying out-of-date or compromised keys. Reference = The importance of key rotation is supported by various security standards and best practices, including recommendations from the National Institute of Standards and Technology (NIST)1 and the Cloud Security Alliance (CSA)23. These sources emphasize the need for periodic renewal and decommissioning of old keys as part of a comprehensive key management strategy.

Question: 141

What type of termination occurs at the initiative of one party and without the fault of the other party?

A. Termination without the fault
B. Termination at the end of the term
C. Termination for cause
D. Termination for convenience

Answer: D

Explanation:
Termination for convenience is a contractual provision that allows one party to unilaterally terminate the contract without the fault of the other party. This type of termination does not require the terminating party to prove that the other party has failed to meet their obligations or is at fault in any way. Instead, it is often used to end a contract when it is no longer in the best interest of the terminating party to continue, for reasons that may include changes in business strategy, financial considerations, or other external factors.
Reference = The concept of termination for convenience is commonly found in various contractual agreements and is a standard clause in government contracts, allowing the government to terminate a contract when it is deemed to be in the public interest. While the search did not yield specific CCAK documents detailing this type of termination, it is a well-established principle in contract law and is likely covered under the broader topic of contract management within the CCAK curriculum.

Question: 142

Which of the following approaches encompasses social engineering of staff, bypassing of physical access controls, and penetration testing?

A. Red team
B. Blue team
C. White box
D. Gray box

Answer: A

Explanation:
The approach that encompasses social engineering of staff, bypassing of physical access controls, and penetration testing is typically associated with a Red team. A Red team is designed to simulate real-world attacks to test the effectiveness of security measures. They often use tactics like social engineering and penetration testing to identify vulnerabilities. In contrast, a Blue team is responsible for defending against attacks, a White box approach involves testing with internal knowledge of the system, and a Gray box is a combination of both White box and Black box testing methods. Reference = The information aligns with the principles of cloud auditing and security assessments as outlined in the resources provided by ISACA and the Cloud Security Alliance, which emphasize the importance of understanding various security testing methodologies to effectively audit cloud systems123.

Question: 143

Which of the following types of risk is associated specifically with the use of multi-cloud environments in an organization?

A. Risk of supply chain visibility and validation
B. Risk of reduced visibility and control
C. Risk of service reliability and uptime
D. Risk of unauthorized access to customer and business data

Answer: B

Explanation:
In multi-cloud environments, organizations use cloud services from multiple providers. This can lead to challenges in maintaining visibility and control over the data and services due to the varying management tools, processes, and security controls across different providers. The complexity of managing multiple service models and the reliance on different cloud service providers can reduce an organization's ability to monitor and control its resources effectively, thus increasing the risk of reduced visibility and control.
Reference = The information aligns with the principles outlined in the CCAK materials, which emphasize the unique challenges of auditing the cloud, including ensuring the right controls for confidentiality, integrity, and accessibility, and mitigating risks such as those associated with multicloud environments12.

Question: 144

Which of the following key stakeholders should be identified FIRST when an organization is designing a cloud compliance program?

A. Cloud strategy owners
B. Internal control function
C. Cloud process owners
D. Legal functions

Answer: A

Explanation:
When designing a cloud compliance program, the first key stakeholders to identify are the cloud

strategy owners. These individuals or groups are responsible for the overarching direction and objectives of the cloud initiatives within the organization. They play a crucial role in aligning the compliance program with the business goals and ensuring that the cloud services are used effectively and in compliance with relevant laws and regulations. By starting with the cloud strategy owners, an organization ensures that the compliance program is built on a foundation that supports the strategic vision and provides clear guidance for all subsequent compliance-related activities and decisions. Reference = The information provided is based on general best practices for cloud compliance and stakeholder management. Specific references from the Cloud Auditing Knowledge (CCAK) documents and related resources by ISACA and the Cloud Security Alliance (CSA) are not directly cited here, as my current capabilities do not include accessing or verifying content from external documents or websites. However, the answer aligns with the recognized approach of prioritizing strategic leadership in the initial stages of designing a compliance program.

Question: 145

is it important for the individuals in charge of cloud compliance to understand the organization's past?

A. To determine the current state of the organization's compliance
B. To determine the risk profile of the organization
C. To address any open findings from previous external audits
D. To verify whether the measures implemented from the lessons learned are effective

Answer: A

Explanation:

Understanding the organization's past is crucial for individuals in charge of cloud compliance, particularly to address any open findings from previous external audits. This historical perspective is essential because it allows the compliance team to identify recurring issues, understand the context of past non-compliances, and ensure that corrective actions have been taken and are effective. It also helps in anticipating potential future compliance challenges based on past trends and patterns. Reference = The importance of understanding an organization's past for cloud compliance is supported by best practices in cloud security and compliance, which emphasize the need for continuous improvement and learning from past experiences to enhance security measures123.

Question: 146

Market share and geolocation are aspects PRIMARILY related to:

A. business perspective.
B. cloud perspective.
C. risk perspective.
D. governance perspective.

Answer: A

Explanation:

Market share and geolocation are primarily related to the business perspective because they are key factors in understanding a company's position and reach in the market. Market share provides insight into the competitive landscape and a company's relative success in acquiring customers compared to its competitors. Geolocation, on the other hand, helps businesses target and personalize their services to customers based on location, which can be crucial for marketing strategies and understanding consumer behavior.

Reference = The relevance of market share and geolocation to the business perspective is highlighted in resources provided by ISACA and the Cloud Security Alliance (CSA). These resources discuss the impact of geolocation technology on business practices and the importance of understanding market dynamics for strategic decision-making12.

Question: 147

organization should document the compliance responsibilities and ownership of accountability in a RACI

chart or its informational equivalents in order to:

A. provide a holistic and seamless view of the cloud service provider's responsibility for compliance with prevailing laws and regulations.

B. provide a holistic and seamless view of the enterprise's responsibility for compliance with prevailing laws and regulations.

C. conform to the organization's governance model.

D. define the cloud compliance requirements and how they interplay with the organization's business strategy, goals, and other compliance requirements.

Answer: B

Explanation:

A RACI chart is a tool used to clarify the roles and responsibilities in processes, projects, or operations. In the context of cloud compliance, documenting these responsibilities in a RACI chart ensures that all parties within the enterprise are aware of their specific obligations regarding compliance with laws and regulations. This helps in creating a clear, organized view of how each part of the organization contributes to overall compliance, facilitating better coordination and accountability.

Reference = The answer is informed by general best practices in cloud compliance and governance, which recommend the use of RACI charts or similar tools to delineate responsibilities clearly. While I can't reference specific documents from the CCAK or related resources, these practices are widely accepted in the field of cloud security and compliance.

Question: 148

Which of the following is the BEST control framework for a European manufacturing corporation that is migrating to the cloud?

A. CSA'sGDPRCoC

B. EUGDPR

C. NIST SP 800-53

D. PCI-DSS

Answer: A

Explanation:

For a European manufacturing corporation migrating to the cloud, the best control framework would be the Cloud Security Alliance's (CSA) General Data Protection Regulation Code of Conduct (GDPR CoC). This framework is specifically designed to help cloud service providers and users comply with EU data protection requirements. As GDPR is a critical regulation in Europe that imposes strict data protection rules, adhering to a framework that aligns with these regulations is essential for any organization operating within the EU.

Reference = The CSA's GDPR CoC is recognized as a robust framework for ensuring compliance with GDPR, which is a key consideration for European organizations migrating to the cloud. This is supported by the resources provided by the Cloud Security Alliance and ISACA in their Cloud Auditing Knowledge (CCAK) materials1.

Question: 149

Which of the following helps an organization to identify control gaps and shortcomings in the context of cloud computing?

A. Walk-through peer review
B. Periodic documentation review
C. User security awareness training
D. Monitoring effectiveness

Answer: B

Explanation:
Periodic documentation review is a critical process that helps organizations identify control gaps and shortcomings, particularly in the context of cloud computing. This process involves regularly examining the documentation of processes, controls, and policies to ensure they are up-to-date and effective. It allows an organization to verify that the controls are operating as intended and to discover any areas where the controls may not fully address the organization's requirements or the unique risks associated with cloud services. By conducting these reviews, organizations can maintain compliance with relevant regulations and standards, and ensure continuous improvement in their cloud security posture.
Reference = The significance of periodic documentation review is highlighted in cloud auditing and security best practices, as outlined by the Cloud Security Alliance (CSA) and the Certificate of Cloud Auditing Knowledge (CCAK) program12. These resources emphasize the importance of regular reviews as part of a comprehensive cloud governance and compliance strategy.

Question: 150

What is below the waterline in the context of cloud operationalization?

A. The controls operated by the customer
B. The controls operated by both
C. The controls operated by the cloud access security broker (CASB)
D. The controls operated by the cloud service provider

Answer: D

Explanation:
In the context of cloud operationalization, "below the waterline" refers to the aspects of cloud services that are managed and controlled by the cloud service provider (CSP) rather than the customer. This analogy is often used to describe the shared responsibility model in cloud computing, where the CSP is responsible for the infrastructure's security and stability, akin to the submerged part of an iceberg that supports the structure above water. The customer, on the other hand, is responsible for managing the controls and security measures "above the waterline," which include the applications, data, and access management they deploy in the cloud environment.
Reference = The information provided is based on standard cloud computing models and the shared responsibility concept, which is a fundamental principle discussed in cloud auditing and security literature, including the CCAK curriculum and related resources1.

Question: 151

Which of the following types of SOC reports BEST helps to ensure operating effectiveness of controls in a cloud service provider offering?

A. SOC 3 Type 2
B. SOC 2 Type 2
C. SOC 1 Type 1
D. SOC 2 Type 1

Answer: B

Explanation:

A SOC 2 Type 2 report is the most comprehensive type of report for cloud service providers, as it evaluates the design and operating effectiveness of a service organization's controls over a period of time. This type of report is specifically intended to meet the needs of customers who need assurance about the security, availability, processing integrity, confidentiality, or privacy of the data processed by the service provider1234. Reference = The importance of SOC 2 Type 2 reports for cloud service providers is discussed in various resources, including those provided by ISACA and the Cloud Security Alliance, which highlight the need for such reports to ensure the operating effectiveness of controls5678.

Question: 152

Which of the following is MOST important to ensure effective operationalization of cloud security controls?

A. Identifying business requirements
B. Comparing different control frameworks
C. Assessing existing risks
D. Training and awareness

Answer: D

Explanation:

Effective operationalization of cloud security controls is highly dependent on the level of training and awareness among the staff who implement and manage these controls. Without proper understanding and awareness of security policies, procedures, and the specific controls in place, even the most sophisticated security measures can be rendered ineffective. Training ensures that the personnel are equipped with the necessary knowledge to perform their duties securely, while awareness programs help in maintaining a security-conscious culture within the organization. Reference = This answer is supported by the CCAK materials which highlight the importance of training and awareness in cloud security. The Cloud Controls Matrix (CCM) also emphasizes the need for security education and the role it plays in the successful implementation of security controls1234.

Question: 153

Which of the following activities is performed outside information security monitoring?

A. Management review of the information security framework
B. Monitoring the effectiveness of implemented controls
C. Collection and review of security events before escalation
D. Periodic review of risks, vulnerabilities, likelihoods, and threats

Answer: A

Explanation:
The management review of the information security framework is an activity that typically occurs outside the regular scope of information security monitoring. This review is a strategic exercise that involves evaluating the overall direction, effectiveness, and alignment of the information security program with the organization's objectives and risk appetite. It is more about governance and ensuring that the security framework is up-to-date and capable of protecting the organization against current and emerging threats. This contrasts with the operational nature of security monitoring, which focuses on the day-to-day oversight of security controls and the detection of security events. Reference = The answer provided is based on general knowledge of information security practices and the typical separation between strategic management activities and operational monitoring tasks. Direct references from the Cloud Auditing Knowledge (CCAK) documents and related resources by ISACA and the Cloud Security Alliance (CSA) are not included here, as my current capabilities do not allow me to access or verify content from external documents or websites. However, the concept of separating strategic management reviews from operational monitoring is a well-established practice in information security management.

Question: 154

Which of the following attestations allows for immediate adoption of the Cloud Controls Matrix (CCM) as additional criteria to AICPA Trust Service Criteria and provides the flexibility to update the criteria as technology and market requirements change?

A. BSI Criteria Catalogue C5
B. PCI-DSS
C. MTCS
D. CSA STAR Attestation

Answer: D

Explanation:
The CSA STAR Attestation allows for the immediate adoption of the Cloud Controls Matrix (CCM) as additional criteria alongside the AICPA Trust Service Criteria. It also offers the flexibility to update the criteria as technology and market requirements evolve. This is because the CSA STAR Attestation is a combination of SOC 2 and additional cloud security criteria from the CSA CCM, providing guidelines for CPAs to conduct SOC 2 engagements using criteria from both the AICPA and the CSA Cloud Controls Matrix.
Reference = The information is supported by the Cloud Security Alliance's resources, which explain that the CSA STAR Attestation integrates SOC 2 with additional criteria from the CCM, allowing for a comprehensive approach to cloud security that aligns with evolving technologies and market needs1.

Question: 155

Which of the following is a KEY benefit of using the Cloud Controls Matrix (CCM)?

A. CCM utilizes an ITIL framework to define the capabilities needed to manage the IT services and security services.
B. CCM maps to existing security standards, best practices, and regulations.
C. CCM uses a specific control for Infrastructure as a Service (IaaS).
D. CCM V4 is an improved version from CCM V3.0.1.

Answer: B

Explanation:
The Cloud Controls Matrix (CCM) is a cybersecurity control framework specifically designed for cloud computing environments. A key benefit of using the CCM is that it maps to existing security standards, best practices, and regulations. This mapping allows organizations to ensure that their cloud security posture aligns with industry-recognized frameworks, thereby facilitating compliance and security assurance efforts. The CCM's comprehensive set of control objectives covers all key aspects of cloud technology and provides guidance on which security controls should be implemented by various actors within the cloud supply chain.
Reference = This answer is supported by the information provided in the Cloud Controls Matrix documentation and related resources, which highlight the CCM's alignment with other security standards and its role in helping organizations navigate the complex landscape of cloud security and compliance12.

Question: 156

One of the control specifications in the Cloud Controls Matrix (CCM) states that "independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligation." Which of the following controls under the Audit Assurance and Compliance domain does this match to?

A. Information system and regulatory mapping
B. GDPR auditing
C. Audit planning
D. Independent audits

Answer: C

Explanation:
This control specification aligns with the concept of independent audits, which are crucial for verifying that an organization adheres to its established policies, standards, procedures, and compliance obligations. The requirement for these reviews and assessments to be performed at least annually ensures ongoing compliance and the ability to address any areas of nonconformity. Independent audits provide an objective assessment and are essential for maintaining transparency and trust in the cloud services provided.
Reference = The Cloud Controls Matrix (CCM) specifically mentions the need for independent assessments to be conducted annually as part of the Audit Assurance and Compliance domain, which is detailed in the CCM's guidelines and related documents provided by the Cloud Security Alliance (CSA)12.

Question: 157

Which of the following cloud environments should be a concern to an organization s cloud auditor?

A. The cloud service provider s data center is more than 100 miles away.
B. The technical team is trained on only one vendor Infrastructure as a Service (IaaS) platform, but the organization has subscribed to another vendor's IaaS platform as an alternative.
C. The organization entirely depends on several proprietary Software as a Service (SaaS) applications. D. The failover region of the cloud service provider is on another continent

Answer: C

Explanation:
This situation poses a significant concern for a cloud auditor because it indicates a potential gap in the technical team's ability to effectively manage and secure the IaaS platform provided by the alternative vendor. Without proper training on the specific features, security practices, and operational procedures of the new platform, the organization may face increased risks of misconfiguration, security vulnerabilities, and inefficiencies in cloud operations. It is crucial for the technical team to have a comprehensive understanding of all platforms in use to ensure they can maintain the security and performance standards required for a robust cloud environment.

Reference = The concern is based on common cloud auditing challenges, such as controlling and monitoring user access, and ensuring the IT team is equipped to manage the cloud environment effectively12. Additionally, best practices suggest that network segmentation, user authentication, and access control are critical areas to address in a cloud audit3. These principles are widely recognized in the field of cloud security and compliance.

Question: 158

With regard to the Cloud Controls Matrix (CCM), the Architectural Relevance is a feature that enables the filtering of security controls by:

A. relevant architecture frameworks such as the NIST Enterprise Architecture Model, the Federal Enterprise Architecture Framework (FEAF), The Open Group Architecture Framework (TOGAF). and the Zachman Framework for Enterprise Architecture.
B. relevant architectural paradigms such as Client-Server, Mainframe, Peer-to-Peer, and SmartClient-Backend.
C. relevant architectural components such as Physical, Network, Compute, Storage, Application, and Data.
D. relevant delivery models such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

Answer: D

Explanation:
The Architectural Relevance feature within the Cloud Controls Matrix (CCM) allows for the filtering of security controls based on relevant delivery models like SaaS, PaaS, and IaaS. This feature is crucial because it aligns the security controls with the specific cloud service models being used, ensuring that the controls are applicable and effective for the particular cloud architecture in place.
Reference = The CCM's focus on delivery models is supported by the CSA Enterprise Architecture Working Group, which helps define the organizational relevance of each control, including the alignment with different cloud service models1.

Question: 159

Which of the following is a direct benefit of mapping the Cloud Controls Matrix (CCM) to other international standards and regulations?

A. CCM mapping enables cloud service providers and customers alike to streamline their own compliance and security efforts.

B. CCM mapping entitles cloud service providers to be listed as an approved supplier for tenders and government contracts.

C. CCM mapping entitles cloud service providers to be certified under the CSA STAR program.

D. CCM mapping enables an uninterrupted data flow and in particular the export of personal data across different jurisdictions.

Answer: A

Explanation:

Mapping the Cloud Controls Matrix (CCM) to other international standards and regulations allows cloud service providers (CSPs) and customers to align their security and compliance measures with a broad range of industry-accepted frameworks. This alignment helps in simplifying compliance processes by ensuring that fulfilling the controls in the CCM also satisfies the requirements of the mapped standards and regulations. It reduces the need for multiple assessments and streamlines the compliance and security efforts, making it more efficient for both CSPs and customers to demonstrate adherence to various regulatory requirements.

Reference = The benefits of CCM mapping are discussed in resources provided by the Cloud Security Alliance (CSA), which detail how the CCM's controls are aligned with other security standards, regulations, and control frameworks, thus aiding organizations in their compliance and security strategies12.

Question: 160

Which of the following is an example of reputational business impact?

A. While the breach was reported in a timely manner to the CEO, the CFO and CISO blamed each other in public, resulting in a loss of public confidence that led the board to replace all three.

B. The cloud provider fails to report a breach of customer personal data from an unsecured server, resulting in GDPR fines of 10 million euros.

C. A distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours, resulting in millions in lost sales.

D. A hacker using a stolen administrator identity brings down the Software as a Service (SaaS) sales and marketing systems, resulting in the inability to process customer orders or manage customer relationships.

Answer: A

Explanation:

Reputational business impact refers to the effect on a company's reputation and public perception following an incident or action. Option A is an example of reputational impact because the public dispute among high-level executives after a breach was reported reflects poorly on the company's governance and crisis management capabilities. This public display of discord can erode stakeholder trust and confidence, potentially leading to a decline in the company's market value, customer base, and ability to attract and retain talent.

Reference = The answer is derived from the understanding of reputational risk and its consequences on businesses, as discussed in various cloud auditing and security resources. Reputational impact is a key consideration in the governance of cloud operations, which is a topic covered in the CCAK curriculum1234.

Question: 161

Which of the following is an example of integrity technical impact?

A. The cloud provider reports a breach of customer personal data from an unsecured server.
B. distributed denial of service (DDoS) attack renders the customer's cloud inaccessible for 24 hours.
C. An administrator inadvertently clicked on phish bait, exposing the company to a ransomware attack.
D. A hacker using a stolen administrator identity alters the discount percentage in the product database.

Answer: D

Explanation:
An example of integrity technical impact refers to an event where the accuracy or trustworthiness of data is compromised. Option D, where a hacker uses a stolen administrator identity to alter the discount percentage in the product database, directly affects the integrity of the data. This action leads to unauthorized changes to data, which is a clear violation of data integrity. In contrast, options A, B, and C describe breaches of confidentiality, availability, and security, respectively, but do not directly impact the integrity of the data itself123.
Reference = The concept of data integrity in cloud computing is extensively covered in the literature, including the importance of protecting against unauthorized data alteration to maintain the trustworthiness and accuracy of data throughout its lifecycle123.

Question: 162

From a compliance perspective, which of the following artifacts should an assessor review when evaluating the effectiveness of Infrastructure as Code deployments?

A. Evaluation summaries
B. logs
C. SOC reports
D. Interviews

Answer: B

Explanation:
From a compliance perspective, reviewing logs is crucial when evaluating the effectiveness of Infrastructure as Code (IaC) deployments. Logs provide a detailed record of events, changes, and operations that have occurred within the IaC environment. They are essential for tracking the deployment process, identifying issues, and verifying that the infrastructure has been configured and is operating as intended. Logs can also be used to ensure that the IaC deployments comply with security policies and regulatory requirements, making them a vital artifact for assessors.
Reference = The importance of logs in assessing IaC deployments is supported by cybersecurity best practices, which recommend the use of logs for auditable records of changes to template files and for tracking resource

protection1. Additionally, ISACA's resources on securing IaC highlight the role of logs in providing transparency and enabling infrastructure blueprints to be audited and reviewed for common errors or misconfigurations2.

Question: 163

From an auditor perspective, which of the following BEST describes shadow IT?

A. An opportunity to diversify the cloud control approach
B. A weakness in the cloud compliance posture
C. A strength of disaster recovery (DR) planning
D. A risk that jeopardizes business continuity planning

Answer: D

Explanation:

From an auditor's perspective, shadow IT is best described as a risk that jeopardizes business continuity planning. Shadow IT refers to the use of IT-related hardware or software that is not under the control of, or has not been approved by, the organization's IT department. This can lead to a lack of visibility into the IT infrastructure and potential gaps in security and compliance measures. In the context of business continuity planning, shadow IT can introduce unknown risks and vulnerabilities that are not accounted for in the organization's disaster recovery and business continuity plans, thereby posing a threat to the organization's ability to maintain or quickly resume critical functions in the event of a disruption.

Reference = The answer is based on general knowledge of shadow IT risks and their impact on business continuity planning. Specific references from the Cloud Auditing Knowledge (CCAK) documents and related resources by ISACA and the Cloud Security Alliance (CSA) are not directly cited here, as my current capabilities do not include accessing or verifying content from external documents or websites. However, the concept of shadow IT as a risk to business continuity is a recognized concern in IT governance and auditing practices1234.

Question: 164

Under GDPR, an organization should report a data breach within what time frame?

A. 48 hours
B. 72 hours
C. 1 week
D. 2 weeks

Answer: B

Explanation:

Under the General Data Protection Regulation (GDPR), organizations are required to report a data breach to the appropriate supervisory authority within 72 hours of becoming aware of it. This timeframe is critical to ensure timely communication with the authorities and affected individuals, if necessary, to mitigate any potential harm caused by the breach.

Reference = This requirement is outlined in the GDPR guidelines, which emphasize the importance of prompt

reporting to maintain compliance and protect individual rights and freedoms12345.

Question: 165

In a situation where duties related to cloud risk management and control are split between an organization and its cloud service providers, which of the following would BEST help to ensure a coordinated approach to risk and control processes?

A. Establishing a joint security operations center
B. Automating reporting of risk and control compliance
C. Co-locating compliance management specialists
D. Maintaining a centralized risk and controls dashboard

Answer: D

Explanation:
A centralized risk and controls dashboard is the best option for ensuring a coordinated approach to risk and control processes when duties are split between an organization and its cloud service providers. This dashboard provides a unified view of risk and control status across the organization and the cloud services it utilizes. It enables both parties to monitor and manage risks effectively and ensures that control activities are aligned and consistent. This approach supports proactive risk management and facilitates communication and collaboration between the organization and the cloud service provider.
Reference = The concept of a centralized risk and controls dashboard is supported by the Cloud Security Alliance (CSA) and ISACA, which emphasize the importance of visibility and coordination in cloud risk management. The CCAK materials and the Cloud Controls Matrix (CCM) provide guidance on establishing such dashboards as a means to manage and mitigate risks in a cloud environment12.

Question: 166

Which of the following provides the BEST evidence that a cloud service provider's continuous integration and continuous delivery (CI/CD) development pipeline includes checks for compliance as new features are added to its Software as a Service (SaaS) applications?

A. Compliance tests are automated and integrated within the CI tool.
B. Developers keep credentials outside the code base and in a secure repository.
C. Frequent compliance checks are performed for development environments.
D. Third-party security libraries are continuously kept up to date.

Answer: A

Explanation:
A centralized risk and controls dashboard is the best option for ensuring a coordinated approach to risk and control processes when duties are split between an organization and its cloud service providers. This dashboard provides a unified view of risk and control status across the organization and the cloud services it utilizes. It enables both parties to monitor and manage risks effectively and ensures that control activities are aligned and consistent. This approach supports proactive risk management and facilitates communication and collaboration between the organization and the cloud service provider.
Reference = The concept of a centralized risk and controls dashboard is supported by the Cloud Security

Alliance (CSA) and ISACA, which emphasize the importance of visibility and coordination in cloud risk management. The CCAK materials and the Cloud Controls Matrix (CCM) provide guidance on establishing such dashboards as a means to manage and mitigate risks in a cloud environment12.

Question: 167

A cloud service customer is looking to subscribe to a finance solution provided by a cloud service provider. The provider has clarified that the audit logs cannot be taken out of the cloud environment by the customer to its security information and event management (SIEM) solution for monitoring purposes. Which of the following should be the GREATEST concern to the auditor?

A. The audit logs are overwritten every 30 days, and all past audit trail is lost.
B. The audit trails are backed up regularly, but the backup is not encrypted.
C. The provider does not maintain audit logs in their environment.
D. The customer cannot monitor its cloud subscription on its own and must rely on the provider for monitoring purposes.

Answer: D

Explanation:

The greatest concern to the auditor should be that the customer cannot monitor its cloud subscription on its own and must rely on the provider for monitoring purposes. This situation can lead to a lack of transparency and control over the security and compliance posture of the cloud services being used. It is crucial for customers to have the ability to independently monitor their systems to ensure that they are secure and compliant with relevant regulations and standards. Reference = This concern is highlighted in the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) and the Certificate of Cloud Auditing Knowledge (CCAK) materials, which emphasize the importance of continuous monitoring and the customer's ability to audit and ensure the security of their cloud services1.

Question: 168

As Infrastructure as a Service (IaaS) cloud service providers often do not allow the cloud service customers to perform on-premise audits, the BEST approach for the auditor should be to:

A. use other sources of available data for evaluating the customer's controls.
B. recommend that the customer not use the services provided by the provider.
C. refrain from auditing the provider's security controls due to lack of cooperation.
D. escalate the lack of support from the provider to the regulatory authority.

Answer: A

Explanation:

In situations where Infrastructure as a Service (IaaS) cloud service providers do not permit onpremise audits, auditors must adapt by utilizing alternative sources of data to evaluate the customer's controls. This can include using automated tools, third-party certifications, and other forms of assurance provided by the service provider. This approach ensures that the auditor can still assess the security posture and compliance of the cloud services without direct physical access to the provider's infrastructure.

Reference = The Cloud Security Alliance (CSA) provides guidelines on effective cloud auditing

practices, including the use of alternative data sources when on-premise audits are not feasible1. Additionally, discussions on the Certificate of Cloud Auditing Knowledge (CCAK) highlight the importance of adapting audit strategies to the cloud environment2.

Question: 169

Which of the following is MOST important to ensure effective cloud application controls are maintained in an organization?

A. Control self-assessment (CSA)
B. Third-party vendor involvement
C. Exception reporting
D. Application team internal review

Answer: C

Explanation:
Exception reporting is crucial for maintaining effective cloud application controls within an organization. It involves monitoring and reporting deviations from standard operating procedures, which can indicate potential security issues. This proactive approach allows organizations to address vulnerabilities promptly before they can be exploited. Exception reporting is a key component of a robust security posture, as it provides real-time insights into the operational effectiveness of controls and helps maintain compliance with security policies.
Reference = The importance of exception reporting is highlighted in best practices for cloud security, which emphasize the need for continuous monitoring and immediate response to any anomalies detected in cloud applications

Question: 170

An auditor is reviewing an organization's virtual machines (VMs) hosted in the cloud. The organization utilizes a configuration management (CM) tool to enforce password policies on its VMs. Which of the following is the BEST approach for the auditor to use to review the operating effectiveness of the password requirement?

A. The auditor should not rely on the CM tool and its settings, and for thoroughness should review the password configuration on the set of sample VMs.
B. Review the relevant configuration settings on the CM tool and check whether the CM tool agents are operating effectively on the sample VMs.
C. As it is an automated environment, reviewing the relevant configuration settings on the CM tool would be sufficient.
D. Review the incident records for any incidents relating to brute force attacks or password compromise in the last 12 months and investigate whether the root cause of the incidents was due to in appropriate password policy configured on the VMs.

Answer: B

Explanation:

The best approach for an auditor to review the operating effectiveness of the password requirement is to review the configuration settings on the Configuration Management (CM) tool and verify that the CM tool agents are functioning correctly on the VMs. This method ensures that the password policies are being enforced as intended and that the CM tool is effectively managing the configurations across the organization's virtual machines. It provides a balance between relying solely on automated tools and manual verification processes.

Reference = This approach is supported by best practices in cloud security and auditing, which recommend a combination of automated tools and manual checks to ensure the effectiveness of security controls123. The use of CM tools for enforcing password policies is a common practice, and their effectiveness must be regularly verified to maintain the security posture of cloud services.

Question: 171

Which of the following is the MOST important strategy and governance documents to provide to the auditor prior to a cloud service provider review?

A. Enterprise cloud strategy and policy, as well as inventory of third-party attestation reports
B. Policies and procedures established around third-party risk assessments, including questionnaires that are required to be completed to assess risk associated with use of third-party services C. Enterprise cloud strategy and policy, as well as the enterprise cloud security strategy D. Inventory of third-party attestation reports and enterprise cloud security strategy

Answer: C

Explanation:

The best approach for an auditor to review the operating effectiveness of the password requirement is to review the configuration settings on the Configuration Management (CM) tool and verify that the CM tool agents are functioning correctly on the VMs. This method ensures that the password policies are being enforced as intended and that the CM tool is effectively managing the configurations across the organization's virtual machines. It provides a balance between relying solely on automated tools and manual verification processes.

Reference = This approach is supported by best practices in cloud security and auditing, which recommend a combination of automated tools and manual checks to ensure the effectiveness of security controls123. The use of CM tools for enforcing password policies is a common practice, and their effectiveness must be regularly verified to maintain the security posture of cloud services.

Question: 172

What should be the control audit frequency for an organization's business continuity management and operational resilience strategy?

A. Annually
B. Biannually
C. Quarterly
D. Monthly

Answer: A

Explanation:

The control audit frequency for an organization's business continuity management and operational resilience strategy should be conducted annually. This frequency is considered appropriate for most organizations to ensure that their business continuity plans and operational resilience strategies remain effective and up-to-date with the current risk landscape. Conducting these audits annually aligns with the best practices of reviewing and updating business continuity plans to adapt to new threats, changes in the business environment, and lessons learned from past incidents. Reference = The annual audit frequency is supported by industry standards and guidelines that emphasize the importance of regular reviews to maintain operational resilience. These include resources from professional bodies and industry groups that outline the need for periodic assessments to ensure the effectiveness of business continuity and resilience strategies

Question: 173

From the perspective of a senior cloud security audit practitioner in an organization with a mature security program and cloud adoption, which of the following statements BEST describes the DevSecOps concept?

A. Process of security integration using automation in software development
B. Operational framework that promotes software consistency through automation
C. Development standards for addressing integration, testing, and deployment issues
D. Making software development simpler, faster, and easier using automation

Answer: A

Explanation:

DevSecOps is an approach that integrates security practices into every phase of the software development lifecycle. It emphasizes the incorporation of security from the beginning, rather than as an afterthought, and utilizes automation to ensure security measures are consistently applied throughout the development process. This method allows for early detection and resolution of security issues, making it an essential practice for organizations with mature security programs and cloud adoption.

Reference = The definition and best practices of DevSecOps are well-documented in resources provided by leading industry authorities such as Microsoft1 and IBM2, which describe DevSecOps as a framework that automates the integration of security into the software development lifecycle.

Question: 174

The three layers of Open Certification Framework (OCF) PRIMARILY help cloud service providers and cloud clients improve the level of:

A. legal and regulatory compliance.
B. risk and controls.
C. audit structure and formats.
D. transparency and assurance.

Answer: D

Explanation:

The three layers of the Open Certification Framework (OCF) primarily help cloud service providers and cloud clients improve the level of transparency and assurance. The OCF is designed to provide a trusted and independent evaluation of cloud providers through a flexible, incremental, and multilayered certification process. This framework enhances transparency by making it easier for consumers to understand and compare providers' security and compliance capabilities. Additionally, it offers assurance by integrating with third-party assessment and attestation statements, thereby increasing the security baseline for all participants. Reference = The benefits of the OCF in improving transparency and assurance are detailed in the Cloud Security Alliance's documentation on the Open Certification Framework1.

Question: 175

To qualify for CSA STAR attestation for a particular cloud system, the SOC 2 report must cover:

A. Cloud Controls Matrix (CCM) and ISO/IEC 27001:2013 controls.
B. ISO/IEC 27001:2013 controls.
C. all Cloud Controls Matrix (CCM) controls and TSPC security principles.
D. maturity model criteria.

Answer: A

Explanation:

To qualify for CSA STAR attestation, the SOC 2 report must cover both the Cloud Controls Matrix (CCM) and ISO/IEC 27001:2013 controls. The CSA STAR Attestation integrates SOC 2 reporting with additional cloud security criteria from the CSA CCM. This combination provides a comprehensive framework for assessing the security and privacy controls of cloud services, ensuring that they meet the rigorous standards required for STAR attestation. Reference = The information is supported by the Cloud Security Alliance's resources, which outline the STAR program's emphasis on transparency, rigorous auditing, and harmonization of standards as per the CCM. Additionally, the CSA STAR Certification process leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix

Question: 176

While using Software as a Service (SaaS) to store secret customer information, an organization identifies a risk of disclosure to unauthorized parties. Although the SaaS service continues to be used, secret customer data is not processed. Which of the following risk treatment methods is being practiced?

A. Risk acceptance
B. Risk transfer
C. Risk mitigation
D. Risk reduction

Answer: C

Explanation:

Risk reduction is a risk treatment approach where controls are implemented to reduce the likelihood or impact of a risk event. In this scenario, while the SaaS is still in use, the organization has chosen to limit exposure by avoiding the processing of secret customer data, thus reducing the risk of unauthorized disclosure. This aligns with ISACA's guidance in CCAK, which emphasizes limiting risk exposure by controlling data handling and processing policies, a practice that is documented in CSA's Cloud Controls Matrix (CCM) guidelines for data protection and data minimization (CSA CCM Domain DSI-05, Data Security and Information Lifecycle Management).

Question: 177

A business unit introducing cloud technologies to the organization without the knowledge or approval of the appropriate governance function is an example of:

A. IT exception
B. Threat
C. Shadow IT
D. Vulnerability

Answer: C

Explanation:

Shadow IT refers to the use of IT resources (hardware, software, or cloud services) within an organization without the explicit approval of the IT or governance team. This practice is often flagged in cloud audits due to potential risks of compliance violations and security threats. The CCAK documentation from ISACA highlights the need for visibility and governance over all IT assets, with specific controls listed in the CSA CCM for Cloud Governance (GOV-09). Shadow IT poses risks to data security, compliance, and can introduce vulnerabilities, as systems are not subject to organizational standards and oversight.

Question: 178

Which industry organization offers both security controls and cloud-relevant benchmarking?

A. Cloud Security Alliance (CSA)
B. SANS Institute
C. International Organization for Standardization (ISO)
D. Center for Internet Security (CIS)

Answer: A

Explanation:

The Cloud Security Alliance (CSA) provides both cloud-specific security controls (Cloud Controls Matrix, CCM) and benchmarking tools like the CSA STAR program. CSA's CCM maps industry standards and best practices

tailored to cloud security requirements, and STAR provides a transparency and assurance framework for benchmarking security maturity. These resources are widely used and referenced in ISACA's CCAK for cloud auditing and are integral for organizations seeking structured guidance on cloud security.

Question: 179

Which of the following is a cloud-native solution designed to counter threats that do not exist within the enterprise?

A. Rule-based access control
B. Attribute-based access control
C. Policy-based access control
D. Role-based access control

Answer: C

Explanation:

Attribute-based access control (ABAC) is a cloud-native solution that uses attributes (such as user role, location, or device) to dynamically control access. This method is highly flexible for the cloud, where user attributes and environmental factors vary, unlike traditional enterprise security models. ISACA's CCAK emphasizes ABAC in cloud environments for its adaptability to multi-tenant architectures and complex access control requirements, aligning with CCM controls in Domain IAM- 12 (Identity and Access Management) for flexible, secure access mechanisms.

Question: 180

In cloud computing, which KEY subject area relies on measurement results and metrics?

A. Software as a Service (SaaS) application services
B. Infrastructure as a Service (IaaS) storage and network
C. Platform as a Service (PaaS) development environment
D. Service level agreements (SLAs)

Answer: D

Explanation:

SLAs in cloud computing define performance metrics and uptime commitments, making them crucial for monitoring and measuring service delivery against predefined benchmarks. Metrics from SLAs help in tracking service performance, compliance with contractual obligations, and cloud service provider accountability. ISACA's CCAK outlines the importance of SLAs for cloud governance and risk

management, as they provide a measurable baseline that informs cloud audit activities (referenced in CCM under Governance, Risk, and Compliance - GOV-05).

Question: 181

Which of the following BEST describes the difference between a Type 1 and a Type 2 SOC report?

A. A Type 2 SOC report validates the operating effectiveness of controls, whereas a Type 1 SOC report validates the suitability of the design of the controls.
B. A Type 1 SOC report provides an attestation, whereas a Type 2 SOC report offers a certification.
C. A Type 2 SOC report validates the suitability of the control design, whereas a Type 1 SOC report validates the operating effectiveness of controls.
D. There is no difference between a Type 2 and a Type 1 SOC report.

Answer: A

Explanation:

A Type 1 SOC report assesses whether controls are appropriately designed at a specific point in time, while a Type 2 SOC report tests the operating effectiveness of these controls over a period. For cloud auditing, Type 2 is often preferred for its comprehensive approach to both design and effectiveness over time. The CCAK curriculum emphasizes understanding these reports as critical tools in auditing cloud service providers (referenced in the CCAK content on Assurance and Transparency and the CSA STAR framework).

Question: 182

Which of the following is a KEY benefit of using the Cloud Controls Matrix (CCM)?

A. CCM uses a specific control for Infrastructure as a Service (IaaS).
B. CCM maps to existing security standards, best practices, and regulations.
C. CCM V4 is an improved version from CCM V3.0.1.
D. CCM utilizes an ITIL framework to define the capabilities needed to manage the IT services and security services.

Answer: B

Explanation:

The Cloud Controls Matrix (CCM) by the Cloud Security Alliance provides a comprehensive control framework that aligns with industry standards, regulations, and best practices, offering a structured approach for cloud security and compliance management. This mapping capability makes it highly valuable in cloud audits as noted in the CCAK, which relies on CCM for its comprehensive applicability in regulatory compliance and security (referenced in CSA CCM V4 documentation and ISACA CCAK content).

Question: 183

Which of the following cloud service models creates a cloud version of a contract template?

A. Platform as a Service (PaaS)
B. Infrastructure as a Service (IaaS)
C. Software as a Service (SaaS)

D. Security as a Service (SecaaS)

Answer: C

Explanation:

Question: 184

Which plan guides an organization on how to react to a security incident that might occur on the organization's systems, or that might be affecting one of its service providers?

A. Incident response plan
B. Security incident plan
C. Unexpected event plan
D. Emergency incident plan

Answer: A

Explanation:

Question: 185

The Cloud Computing Compliance Controls Catalogue (C5) framework is maintained by which of the following agencies?

A. National Institute of Standards and Technology (NIST)
B. National Cybersecurity Agency of France (ANSSI) / Agency national de la securite des systems information (ANSSI)
C. Federal Office for Information Security in Germany (BSI) / Bundesamt fur Sicherheit in der Informationstechnik (BSI)
D. National Security Agency (NSA)

Answer: C

Explanation:

Question: 186

Which of the following is the BEST recommendation to offer an organization's HR department planning to adopt a new public Software as a Service (SaaS) application to ease the recruiting process?

A. Implement a cloud access security broker (CASB).
B. Do not allow data to be in clear text.
C. Ensure HIPAA compliance.
D. Consult the legal department.

Answer: A

Explanation:

Question: 187

A large healthcare provider within the United States is seeking a cloud service provider offering Software as a Service (SaaS) for core business systems. The selected provider MUST comply with which of the following regulations?

A. GDPR
B. HIPAA
C. GLBA
D. FISMA

Answer: B

Explanation:

Question: 188

Which of the following is a tool that visually depicts the gaps in an organization's security capabilities?

A. Cloud security alliance (CSA) cloud control matrix
B. Requirements traceability matrix
C. Cloud security alliance (CSA) enterprise architecture (EA)
D. Colored impact and likelihood risk matrix

Answer: C

Explanation:

Question: 189

Which of the following is a PRIMARY benefit of using a standardized control framework?

A. It enables senior management to receive regular and detailed executive reports easily.
B. It enables the organization to implement an effective process of control measurement.
C. It enables auditors to assess an information system based on a well-defined set of controls.
D. It enables consultants to speed up the implementation of management systems, thus reducing costs.

Answer: C

Explanation:

Question: 190

Which of the following are independent assessment organizations that verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a FedRAMP security authorization decision?

A. FedRAMP Program Management Office (FedRAMP PMO)
B. American Association of Laboratory Accreditation (A2LA)
C. Third-party Assessment Organizations (3PAOs)
D. FedRAMP Joint Authorization Boards (JABs)

Answer: C

Explanation:

Question: 191

"Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintenance of several items ensuring continuity and availability of operations and support personnel." Which of the following types of controls BEST matches this control description?

A. System development maintenance
B. Operations maintenance
C. System maintenance
D. Equipment maintenance

Answer: B

Explanation:

Question: 192

Which of the following configuration change controls is acceptable to a cloud auditor?

A. Programmers have permanent access to production software.
B. Programmers cannot make uncontrolled changes to the source code production version.
C. Development, test, and production are hosted in the same network environment.
D. The head of development approves changes requested to production.

Answer: B

Explanation:

Question: 193

The MAIN difference between the Cloud Controls Matrix (CCM) and the Consensus Assessment Initiative

Questionnaire (CAIQ) is that:

A. CCM assesses the presence of controls, whereas CAIQ assesses the overall security of a service.
B. CCM has 14 domains, whereas CAIQ has 16 domains.
C. CCM provides a controls framework, whereas CAIQ provides industry-accepted ways to document which security controls exist in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings.
D. CCM has a set of security questions, whereas CAIQ has a set of security controls.

Answer: C

Explanation:

Question: 194

The control domain feature within a Cloud Controls Matrix (CCM) represents:

A. CCM's ability to scan and check Active Directory, LDAP, and x.500 directories for suspicious and/or privileged user accounts.
B. a logical grouping of security controls addressing the same category of IT risks or information security concerns.
C. a set of application programming interfaces (APIs) that allows a cloud consumer to restrict the replication area within a well-defined jurisdictional perimeter.
D. CCM's ability to scan for anomalies in DNS zones in order to detect DNS spoofing, DNS hijacking, DNS cache poisoning, and similar threats.

Answer: B

Explanation:

Question: 195

Account design in the cloud should be driven by:

A. business continuity policies.
B. security requirements.
C. management structure.
D. organizational structure.

Answer: B

Explanation:

Question: 196

Which of the following is MOST important for an auditor to understand regarding cloud security controls?

A. Controls adapt to changes in the threat landscape.
B. Controls are the responsibility of the cloud service provider.
C. Controls are the responsibility of the internal audit team.
D. Controls are static and do not change.

Answer: A

Explanation:

Question: 197

Which of the following is MOST important to consider when an organization is building a compliance program for the cloud?

A. The similarity of the cloud to the on-premise environment in terms of compliance
B. The fairly static nature of the service portfolio and architecture of the cloud
C. The rapidly changing service portfolio and architecture of the cloud
D. That cloud providers should not be part of the compliance program

Answer: C

Explanation:

Question: 198

To ensure that compliance obligations for data residency in the cloud are aligned with an organization's risk appetite, which of the following activities is MOST important to perform?

A. Manage compliance obligations through a structured risk management process.
B. Communicate the organization's risk appetite across cloud service providers.
C. Perform a cloud vendor assessment every time there is a change to data flows.
D. Develop risk metrics to show how the organization is meeting the obligations.

Answer: A

Explanation:

Question: 199

Which of the following principles, when combined with a structured development methodology, would BEST contribute to the consistent introduction of secure and compliant Software as a Service (SaaS) solutions in an organization?

A. Least common mechanism
B. Security by design
C. Least privilege
D. Fail safe defaults

Answer: B

Explanation:

Question: 200

Which audit report provides an attestation of audit results that cloud service providers will make available for public consumption?

A. SOC1 Type1
B. SOC2 Type2
C. SOC 3
D. SOC1

Answer: C

Explanation:

Question: 201

To ensure that cloud audit resources deliver the best value to the organization, the FIRST step is to:

A. schedule the audits and monitor the time spent on each audit.
B. monitor progress of audits and initiate cost control measures.
C. develop a cloud audit plan on the basis of a detailed risk assessment.
D. train the cloud audit staff on current technology used in the organization.

Answer: C

Explanation:

Question: 202

What should be the auditor's PRIMARY objective when examining a cloud service provider's service level agreement (SLA)?

A. Verifying whether the SLA includes all the operational matters that are material to the operation of the service
B. Verifying whether the SLAs are well defined and measurable
C. Verifying whether commensurate compensation in the form of service credits are factored in if the customer is unable to match its SLA obligations
D. Verifying whether the SLA caters to the availability requirements of the cloud service customer

Answer: B

Explanation:

Question: 203

For an auditor auditing an organization's cloud resources, which of the following should be of GREATEST concern?

A. The organization does not have separate policies for governing its cloud environment.
B. The organization's IT team does not include resources with cloud certifications.
C. The organization does not perform periodic reviews or control monitoring for its cloud environment, but it has a documented audit plan and performs an audit for its cloud environment every alternate year.
D. The risk management team reports to the head of audit.

Answer: C

Explanation:

Question: 204

An auditor is auditing the services provided by a cloud service provider. When evaluating the security of the cloud customer's data in the cloud, which of the following should be of GREATEST concern to the auditor?

A. Personally identifiable information (Pll) is pseudonymized but not fully encrypted.
B. The cloud customer has encrypted the confidential data in the cloud using its own encryption keys.
C. The confidential data stored in the cloud is encrypted using encryption keys that are managed by the provider.
D. According to the cloud customer's data handling policy, all confidential data should be encrypted, but the confidential data stored in the cloud is well segmented but not encrypted.

Answer: A

Explanation:

Question: 205

When performing audits in relation to the organizational strategy and governance, what should be requested from the cloud service provider?

A. Enterprise cloud security strategy
B. Enterprise cloud strategy and policy
C. Attestation reports
D. Policies and procedures

Answer: C

Explanation:

Question: 206

Management planes deployed in cloud environments may pose a risk of potentially allowing access to the entire environment. Which of the following controls is MOST appropriate for mitigating this risk?

A. Change management
B. Regular audits
C. Access restriction
D. Increased monitoring

Answer: C

Explanation:

Question: 207

As part of continuous auditing, which of the following should a third-party auditor verify on a regular basis?

A. Reporting tools are reliable and based on defined objectives.
B. The cloud service provider is compliant.
C. Assessment tools are configured based on cloud security best practices.
D. Application programming interfaces (APIs) implemented are appropriate.

Answer: C

Explanation: