Watermark Sample

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"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

A newly established IT steering committee is concerned about whether a system is meeting availability objectives. Which of the following will provide the BEST information to make an assessment?

A. Balanced scorecard
B. Capability maturity levels
C. Performance indicators
D. Critical success factors (CSFs)

Answer: C

Explanation:

Performance indicators are quantitative measures that can be used to evaluate the availability of a system or service. They can include metrics such as uptime, downtime, response time, availability percentage, etc. Balanced scorecard, capability maturity levels, and critical success factors are not directly related to availability objectives, but rather to strategic alignment, process improvement, and goal achievement respectively. Reference := CGEIT Exam Content Outline, Domain 1: Governance of Enterprise IT, Subdomain A: Governance Framework, Task 5: Establish and monitor key performance indicators (KPIs) and key goal indicators (KGIs) that are aligned with strategic objectives.

Question: 2

Which of the following is the BEST method to monitor IT governance effectiveness?

A. Service level management
B. Balanced scorecard
C. Risk control self-assessment (CSA)
D. SWOT analysis

Answer: B

Explanation:

A balanced scorecard is a strategic management tool that measures and monitors the performance of an organization against its vision, mission, goals, and objectives. It uses four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help evaluate the effectiveness of IT governance by aligning IT activities with business strategies,
assessing IT value delivery, identifying IT strengths and weaknesses, and facilitating continuous improvement. Reference := CGEIT Exam Content Outline, Domain 1: Governance of Enterprise IT, Subdomain B: Strategic Management, Task 3: Establish and maintain a framework for the governance of enterprise IT to enable the achievement of enterprise objectives.

Question: 3

An IT audit reveals inconsistent maintenance of data privacy in enterprise systems primarily due to a lack of data sensitivity categorizations. Once the categorizations are defined, what is the BEST longterm strategic response by IT governance to address this problem?

A. Standardize data classification processes throughout the enterprise.
B. Incorporate enterprise privacy categorizations into contracts.
C. Require business impact analyses (BIAs) for enterprise systems.
D. Reassess the data governance policy.

Answer: A

Explanation:

Data classification is the process of categorizing data according to its sensitivity, such as public, confidential, or restricted. Data classification helps ensure that data privacy is maintained by applying appropriate controls and policies to different types of data. By standardizing data classification processes throughout the enterprise, IT governance can ensure consistent and effective data privacy practices across all systems and departments. Incorporating enterprise privacy categorizations into contracts, requiring business impact analyses for enterprise systems, and reassessing the data governance policy are not long-term strategic responses, but rather tactical or operational actions that may support data privacy. Reference := What is Data Classification?, Data Governance Policy: Examples & Templates, What is data governance?

Question: 4

A new and expanding enterprise has recently received a report indicating 90% of its data has been collected in just the last six months, triggering data breach and privacy concerns. What should be the IT steering committee's FIRST course of action to ensure new data is managed effectively?

A. Mitigate and track data-related issues and risks.
B. Modify legal and regulatory data requirements.
C. Define data protection and privacy practices.
D. Assess the information governance framework.

Answer: D

Explanation:

An information governance framework is the structure that provides a holistic overview of the influences that inform how an organisation creates and manages its enterprise-wide information assets (records, information and data)1. It defines the roles, responsibilities, policies, standards, and processes for ensuring effective and secure information management. If a new and expanding enterprise has collected a large amount of data in a short period of time, it may face data breach and privacy risks if it does not have a robust and comprehensive information governance framework in place. Therefore, the IT steering committee's first course of action should be to assess the current state of the information governance framework, identify any gaps or weaknesses, and implement
improvements or changes as needed. This will help the enterprise to protect and preserve its information assets, comply with legal and regulatory requirements, and enable ethical and efficient use of information. Mitigating and tracking data-related issues and risks, modifying legal and regulatory data requirements, and defining data protection and privacy practices are important actions, but they are not the first course of action. They are more likely to be part of the implementation or improvement of the information governance framework after it has been assessed. Reference := Establishing an information governance framework

Question: 5

An enterprise is planning to replace multiple enterprise resource planning (ERP) systems at various regions with one company-wide ERP system. The main objective of this change is to achieve economies of scale efficiencies resulting in cost reductions. To meet this objective, what is the BEST approach in the planning phase of the project?

A. Implement an ERP system on shared resources with the lowest cost.
B. Minimize customization by standardizing ERP processes across regions.
C. Adopt a best in breed web-based architecture for the ERP system.

D. Use a service provider to evaluate and implement the new ERP processes.

Answer: B

Explanation:

One of the main benefits of ERP systems is that they can integrate and streamline various business processes across an enterprise, such as accounting, inventory, sales, human resources, etc. However, this also means that different regions or departments may have to adopt common or standardized processes that are supported by the ERP system, rather than using their own customized or localized ones. This can reduce the complexity and cost of implementing and maintaining the ERP system, as well as improve data quality and consistency. According to one of the web search results1, "it's important to always keep those processes at the core of yourimplementation plan" and "an ERP implementation is an opportunity to introduce a better process, not simply to automate an existing inefficient one." Another web search result2 states that "standardizing ERP processes across regions" is one of the best practices for a successful ERP implementation. Therefore, the best approach in the planning phase of the project is to minimize customization by standardizing ERP processes across regions. Reference := 9 Key ERP Implementation Best Practices | NetSuite, 6 Best Practices for a Successful ERP Implementation

Question: 6

While monitoring an enterprise's IT projects portfolio, it is discovered that a project is 75% complete, but all budgeted resources have been expended. Which of the following is the MOST important task to perform?

A. Review the IT investments.
B. Reorganize the IT projects portfolio.
C. Re-evaluate the business case.
D. Review the IT governance structure.

Answer: C

Explanation:

A business case is a document that justifies the initiation and continuation of a project based on its expected benefits, costs, risks, and alignment with the strategic objectives of the organization. If a project is experiencing a cost overrun, meaning that it has exceeded its initial budget, it is important to re-evaluate the business case to determine whether the project is still viable and worth pursuing. Re-evaluating the business case can help to identify the root causes of the cost overrun, assess the impact of the overrun on the project's value proposition, and decide whether to continue, modify, or terminate the project. Reviewing the IT investments, reorganizing the IT projects portfolio, and reviewing the IT governance structure are not the most important tasks to perform in this situation. They are more likely to be part of the portfolio management or governance processes that should be done regularly or periodically, not in response to a specific project issue. Moreover, they do not directly address the problem of the cost overrun or its implications for the project's feasibility and desirability. Reference := What is a Business Case?, How to Write a Business Case, Project Cost Overruns – Reasons, How to Prevent and Manage

Question: 7

Six months ago, an enterprise's CIO reorganized IT to improve service delivery to the business. Which of the following would BEST demonstrate the effectiveness of the reorganization?

A. The number of help desk calls
B. A balanced scorecard
C. A survey of IT staff
D. IT cost reduction

Answer: B

Explanation:

A balanced scorecard is a strategic management tool that measures and monitors the performance of an organization against its vision, mission, goals, and objectives. It uses four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help demonstrate the effectiveness of the IT reorganization by showing how the IT function has improved in terms of delivering value to the business, satisfying customer needs and expectations, optimizing internal processes and workflows, and enhancing the skills and capabilities of the IT staff. According to one of the web search results1, "a balanced scorecard can help evaluate the effectiveness of IT governance by aligning IT activities with business strategies, assessing IT value delivery, identifying IT strengths and weaknesses, and facilitating continuous improvement." The number of help desk calls, a survey of IT staff, and IT cost reduction are not the best indicators of the effectiveness of the IT reorganization. They are more likely to reflect operational or tactical aspects of IT service delivery, rather than strategic or holistic ones. They may also be influenced by other factors that are not related to the IT reorganization, such as user behavior, staff morale, or market conditions. Reference := Service Delivery for IT and Business | Splunk

Question: 8

An enterprise is evaluating a possible strategic initiative for which IT would be the main driver. There are several risk scenarios associated with the initiative that have been identified. Which of the following should be done FIRST to facilitate a decision?

A. Define the risk mitigation strategy.
B. Assess the impact of each risk.
C. Establish a baseline for each initiative.
D. Select qualified personnel to manage the project.

Answer: B

Explanation:

Before deciding whether to pursue a strategic initiative, it is important to understand the potential consequences of the risks involved. Assessing the impact of each risk means estimating how likely it is to occur and how severe its effects would be on the enterprise's objectives, performance, reputation, or resources. This can help to prioritize the most critical risks and compare them with the expected benefits of the initiative. According to one of the web search results1, "the impact assessment is a key element of any risk management process. It helps to evaluate the significance of each risk and determine the appropriate response strategy." Defining the risk mitigation strategy, establishing a baseline for each initiative, and selecting qualified personnel to manage the project are important steps, but they are not the first ones. They aremore likely to be part of the implementation or execution phase of the initiative, after it has been approved and funded. Reference := Risk Impact Assessment and Prioritization

Question: 9

Enterprise IT has overseen the implementation of an array of data services with overlapping functionality leading to business inefficiencies. Which of the following is the MOST likely cause of this situation?

A. insufficient information architecture
B. Ineffective project management
C. An outdated service level agreement (SLA)
D. An incomplete cost-benefit analysis

Answer: A

Explanation:

Information architecture (IA) is the process of guiding users through the site by organising and arranging all the relevant content in a clear, intuitive way. It also ensures consistency throughout a product's design by standardising labelling conventions such as menu names, link titles, and button labels across all pages1. If enterprise IT has overseen the implementation of an array of data services with overlapping functionality, it may indicate that they have not followed a coherent and effective IA strategy. This can lead to business inefficiencies, such as duplication of efforts, confusion among users, and difficulty in finding and accessing information. According to one of the web search results2, "Application rationalization is a simple first step to analyze the current architecture to determine redundant applications, overlapping functionality, and software that is not exactly current. As more companies move into a service-oriented architecture implementation, this analysis is a cost-effective way to ensure that the IT resources are utilized in the most efficient manner." Ineffective project management, an outdated service level agreement (SLA), and an incomplete costbenefit analysis are not the most likely causes of this situation. They are more related to the planning, execution, and evaluation of individual projects, rather than the overall design and organisation of information systems. Reference := What is information architecture? - UX Design Institute, Staying Current And Supporting Systems With Overlapping Functionality

Question: 10

Which of the following would be the BEST way to facilitate the adoption of strong IT governance practices throughout a multi-divisional enterprise?

A. Ensuring each divisional policy is consistent with corporate policy
B. Ensuring divisional governance fosters continuous improvement processes
C. Mandating data standardization across the distributed enterprise
D. Documenting and communicating key management practices across divisions

Answer: D

Explanation:

Documenting and communicating key management practices across divisions is the best way to facilitate the adoption of strong IT governance practices throughout a multi-divisional enterprise. This can help to ensure that all divisions are aware of and aligned with the corporate IT governance framework, policies, and standards. It can also promote collaboration, coordination, and consistency among the divisions, as well as transparency, accountability, and trust. According to one of the web search results1, "communication is a critical success factor for IT governance implementation" and "effective communication can help to create a shared understanding of IT governance objectives, roles, responsibilities, and benefits among stakeholders." Ensuring each divisional policy is consistent with corporate policy, ensuring divisional governance fosters continuous improvement processes, and mandating data standardization across the distributed enterprise are not the best ways to facilitate the adoption of strong IT governance practices throughout a multi-divisional enterprise. They are more likely to be part of the implementation or improvement of IT governance practices, rather than the facilitation of them. They may also encounter resistance or challenges from the divisions due to different business needs, cultures, or preferences. Reference := IT Governance Practices For Improving Strategic And Operational …

Question: 11

An enterprise considers implementing a system that uses a technology that is not in line with its IT strategy.

The business case indicates significant benefit to the enterprise. Which of the following is the BEST way to manage this situation within an IT governance framework?

A. Update the IT strategy to align with the new technology.
B. Initiate an operational change request.
C. Reject based on non-alignment.
D. Address as part of an architecture exception process.

Answer: D

Explanation:

An architecture exception process is a mechanism to handle requests for deviations from the established IT architecture policies or standards. It allows the enterprise to evaluate the business case, risks, benefits, and alternatives of implementing a system that uses a technology that is not in line with its IT strategy. It also enables the enterprise to define the conditions, limitations, and timelines for granting or denying the exception. According to one of the web search results1, "requests for exceptions to any architectural policy or standard use this process" and "the decision may include a deadline for removing the need for the exception, constraints on future projects, or similar terms." Addressing the situation as part of an architecture exception process is the best way to manage it within an IT governance framework, as it provides a structured andtransparent way to
balance the business needs and the IT alignment. Updating the IT strategy to align with the new technology, initiating an operational change request, or rejecting based on non-alignment are not the best ways to manage the situation within an IT governance framework. They are more likely to be either too rigid or too reactive, and may not consider the trade-offs or implications of the decision..

Reference:

CGEIT Review Manual 2021, Chapter 1: Governance of Enterprise IT, Section 1.4: Value Delivery, page 231
CGEIT Review Questions, Answers & Explanations Manual 2021, Question 9, page 82
A Matrixed Approach to Designing IT Governance - MIT Sloan Management Review3
Enterprise Architecture Governance | The Definitive Guide - LeanIX4
Architecture Review Board Exception Process - Minnesota's State Portal5

Question: 12

Which of the following groups should approve the implementation of new technology?

A. IT steering committee
B. IT audit department
C. Portfolio management office
D. Program management office

Answer: A

Explanation:

An IT steering committee is a group of senior executives who are responsible for directing, reviewing, and approving IT strategic plans, overseeing major initiatives, and allocating resources. They are the most appropriate group to approve the implementation of new technology, as they can ensure that it aligns with the organization's vision, mission, goals, and objectives. They can also evaluate the business case, risks, benefits, and alternatives of the new technology and provide guidance and support to the IT team. According to one of the web search results1, "the steering committee establishes IT priorities for the business as a whole."

Reference := What is an IT Steering Committee? – BMC Software | Blogs

Question: 13

A regulatory audit assessed an enterprise's main transactional application as noncompliant. In addition to fines and required corrections, an agreement was reached to implement a set of governance controls over IT. Accountability for these controls is BEST assigned to which of the following?

A. CIO
B. Internal audit director
C. Application users
D. The board of directors

Answer: D

Explanation:

The board of directors is ultimately responsible for the governance of IT and ensuring that IT supports the enterprise's objectives and strategy. The board of directors should also oversee the implementation and monitoring of IT governance controls to ensure compliance with laws and regulations.
Reference: ISACA, CGEIT Review Manual, 7th Edition, 2019, page 17.

Question: 14

An enterprise can BEST assess the benefits of a new IT project through its life cycle by:

A. calculation of the total cost of ownership.
B. periodic review of the business case.
C. periodic measurement of the project slip rate.
D. calculation of the net present value (NPV).

Answer: B

Explanation:

A business case is a document that outlines the rationale, objectives, benefits, costs, risks and alternatives of a proposed IT project. A business case should be reviewed periodically throughout the project life cycle to ensure that the project is still aligned with the enterprise's strategy and goals, and that the expected benefits are still achievable and realistic. A periodic review of the business case can also help to identify any changes or issues that may affect the project's scope, schedule, budget or quality, and to take corrective actions accordingly.
Reference: ISACA, CGEIT Review Manual, 7th Edition, 2019, page 77. A guide to measuring benefits effectively. Cost-Benefit Analysis: A Quick Guide with Examples and Templates.

Question: 15

The PRIMARY reason for an enterprise to adopt an IT governance framework is to:

A. assure IT sustains and extends the enterprise strategies and objectives.
B. expedite IT investments among other competing business investments.
C. establish IT initiatives focused on the business strategy.
D. allow IT to optimize confidentiality, integrity, and availability of information assets.

Answer: A

Explanation:

IT governance is a framework that provides a formal structure for organizations to ensure that IT investments support business objectives. The primary reason for an enterprise to adopt an ITgovernance framework is to assure that IT sustains and extends the enterprise strategies and objectives, by aligning IT with business needs, optimizing IT performance and value, managing IT risks and resources, and measuring IT outcomes and

benefits12. Reference: ISACA, CGEIT Review Manual, 7th Edition, 2019, page 15. What Is IT Governance? Definition, Practices and Frameworks. IT Governance: Definition, Frameworks, and Best Practices.

Question: 16

Which of the following is the BEST approach when reviewing The security status of a new business acquisition?

A. Embed IT risk management strategies in service level agreements (SLAs).
B. Establish a committee to oversee the alignment of IT security in new businesses.
C. Incorporate IT security objectives to cover additional risks associated with new businesses.
D. Integrate IT risk assessment into the overall due diligence process.

Answer: D

Explanation:

The security status of a new business acquisition is a critical factor that can affect the value, performance, and reputation of the acquiring company. Therefore, it is essential to conduct a thorough IT risk assessment of the target company as part of the overall due diligence process. An IT risk assessment can help to identify and evaluate the current and potential cybersecurity threats, vulnerabilities, and controls in the target company's IT environment, as well as the compliance with relevant laws and regulations. An IT risk assessment can also help to estimate the costs and efforts required to remediate any security gaps or issues, and to align the security policies and standards of both parties. By integrating IT risk assessment into the due diligence process, the acquiring company can make informed decisions about the feasibility, valuation, and integration of the new business acquisition12. Reference: Due diligence for Mergers and Acquisitions through a cybersecurity lens. Microsoft Security tips for mitigating risk in mergers and acquisitions.

Question: 17

The board of directors of an enterprise has approved a three-year IT strategic program to centralize the core business processes of its global entities into one core system. Which of the following should be the ClO's NEXT step?

A. Engage a team to perform a business impact analysis (BIA).
B. Require the development of a risk management plan.
C. Determine resource requirements for program implementation.
D. Require the development of a program roadmap.

Answer: D

Explanation:

A program roadmap is a strategic plan that outlines the vision, objectives, scope, deliverables, milestones, dependencies, risks, and benefits of a large-scale IT program. A program roadmap can help the CIO and other stakeholders to communicate, align, and monitor the progress and outcomes of the program. A program roadmap is essential for a complex and long-term IT program such as centralizing the core business processes of global entities into one core system. A program roadmap can help to ensure that the program is aligned with the IT strategy and the business goals, that the program has a clear and realistic scope and schedule, that the program has adequate resources and governance, and that the program delivers the expected value and benefits1234. Reference: How to Create an IT Strategy Roadmap. Definitive Guide to Developing an IT Strategy and Roadmap. What is an IT Roadmap?. How To Develop a Strategy Roadmap in Six Steps.

Question: 18

Which of the following is the MOST important driver of IT governance?

A. Effective internal controls
B. Management transparency
C. Quality measurement
D. Technical excellence

Answer: B

Explanation:

Management transparency is the most important driver of IT governance, because it enables the alignment of IT and business goals, the accountability of IT performance and value, the communication and collaboration among stakeholders, and the compliance with laws and regulations. Management transparency refers to the degree to which information about IT decisions, processes, outcomes, and risks is shared openly and honestly with relevant parties, such as the board of directors, senior management, business units, IT staff, customers, and regulators. Management transparency can help to build trust, confidence, and support for IT initiatives, as well as to identify and address any issues or gaps in IT governance12. Reference: What is IT governance? A formal way to align IT & business strategy. Definition of IT Governance (ITG) - IT Glossary | Gartner.

Question: 19

A global enterprise is experiencing an economic downturn and is rapidly losing market share. IT senior management is reassessing the core activities of the business, including IT, and the associated resource implications. Management has decided to focus on its local market and to close international operations. A critical issue from a resource management perspective is to retain the most capable staff. This is BEST achieved by:

A. reviewing current goals-based performance appraisals across the enterprise.
B. ranking employees across the enterprise based on their compensation.
C. ranking employees across the enterprise based on length of service.
D. retaining capable staff exclusively from the local market.

Answer: A

Explanation:

Goals-based performance appraisals are a method of evaluating employees based on their achievement of specific and measurable objectives that are aligned with the organization's strategy and vision. Goals-based performance appraisals can help to identify the most capable staff who have contributed to the organization's success, demonstrated high performance and potential, and shown commitment and engagement. Reviewing current goals-based performance appraisals across the enterprise can help management to retain the most capable staff regardless of their location, compensation, or length of service12. Reference: Performance Appraisal Methods: Traditional and Modern Methods (with example). How to Conduct a Performance Appraisal.

Question: 20

An IT steering committee is presented with an audit finding that new software applications are delivered on time but consistently have unacceptable levels of defects. Which of the following would be the BEST direction from the committee?

A. Implement performance indicators.
B. Evaluate the change management process.
C. Establish code peer reviews.
D. Evaluate the quality assurance process.

Answer: D

Explanation:

The quality assurance process is the set of activities that ensures that the software development process follows the defined standards and meets the customer requirements. The quality assurance process includes planning, designing, executing, and monitoring the tests, as well as reporting and resolving the defects. Evaluating the quality assurance process can help to identify and improve the root causes of software defects, such as inadequate testing techniques, tools, or resources, poor communication or collaboration among stakeholders, or lack of quality control or feedback mechanisms123. Reference: QA Process: A Complete Guide to QA Stages, Steps, & Tools. What is Software Quality Assurance (SQA): A Guide for Beginners. Software Quality Assurance | Components | Standards | Techniques - EDUCBA.

Question: 21

A CIO is concerned with the potential of vendor system failures that could cause a large amount of unintended system downtime. To determine how to prepare for this concern, what is MOST important for the CIO to review?

A. IT balanced scorecard
B. Service-level metrics
C. IT procurement policy
D. Business impact analysis (BIA)

Answer: D

Explanation:

A business impact analysis (BIA) is a process of predicting the organizational and financial impact of business disruptions, such as vendor system failures. A BIA can help the CIO to prepare for this concern by identifying the critical business processes, the potential effects of disruption, and the recovery requirements and strategies. A BIA can also help the CIO to prioritize the resources and actions needed to restore the normal operations as quickly as possible1. A BIA is an essential component of business continuity planning (BCP) and disaster recovery planning (DRP)2.

An IT balanced scorecard is a tool that measures and monitors the performance of IT in relation to the strategic goals and objectives of the organization. An IT balanced scorecard can help the CIO to evaluate the effectiveness and efficiency of IT, but it does not address the impact of business disruptions or the recovery plans.

Service-level metrics are indicators that measure and report the quality and availability of IT services delivered to the customers or users. Service-level metrics can help the CIO to track and improve the service delivery, but they do not assess the impact of business disruptions or the recovery plans. An IT procurement policy is a document that defines the rules and procedures for acquiring IT products and services from external vendors. An IT procurement policy can help the CIO to manage the vendor relationships, contracts, and risks, but it does not analyze the impact of business disruptions or the recovery plans. Reference: How To Conduct Business Impact Analysis in 8 Easy Steps. The Top 10 Vendor Risks & How to Manage Them. What is FMEA? Failure Mode & Effects Analysis. Definition of Business Impact Analysis (BIA). [IT Balanced Scorecard: Definition, Frameworks, Examples]. [Service Level Metrics: Definition, Types, Examples]. [IT Procurement Policy: Definition, Components, Examples].

Question: 22

The BEST way to manage continuous improvement of governance-related processes is to: A. assess existing process resource capacities.

B. define accountability based on roles and responsibilities.

C. apply effective quality management practices.
D. require third-party independent reviews.

Answer: C

Explanation:

Quality management is the process of ensuring that the products and services delivered by an organization meet or exceed the expectations and requirements of the customers and stakeholders. Quality management practices include planning, implementing, monitoring, and improving the quality standards and processes for an organization. Applying effective quality management practices can help to manage continuous improvement of governance-related processes, by ensuring that the processes are aligned with the organizational goals and objectives, that the processes are performed consistently and efficiently, that the processes are measured and evaluated for their effectiveness and value, and that the processes are continuously reviewed and enhanced for improvement123. Reference: What is Quality Management? Definition, Principles, Tools & Examples. Quality Management: The Importance of ISO. Continuous Improvement and a Business Process Governance Framework.

Question: 23

Which of the following would BEST enable business innovation through IT?
A. Outsourcing of IT to a strategic business partner
B. Business participation in IT strategy development
C. Adoption of a standardized business development life cycle
D. IT participation in business strategy development

Answer: D

Explanation:

Business innovation is the process of creating new or improved products, services, processes, or business models that create value for the organization and its customers. IT can enable business innovation by providing the tools, platforms, data, and capabilities that support the generation, implementation, and diffusion of innovative ideas. However, IT alone cannot drive business innovation; it requires a close collaboration and alignment between IT and business. Therefore, IT participation in business strategy development is the best way to enable business innovation through IT, because it can help to ensure that IT understands the business goals and needs, that IT contributes to the identification and evaluation of opportunities and challenges, that IT provides feasible and effective solutions and recommendations, and that IT supports the execution and monitoring of the innovation initiatives123. Reference: How to Drive Business Innovation Through IT. How to Enable Business Innovation with IT. Business Innovation: What It Is and How to Achieve It.

Question: 24

Acceptance of an enterprise's newly implemented IT governance initiatives has been resisted by a functional group requesting more autonomy over technology choices. Which of the following is MOST important to accommodate this need for autonomy?
A. Continuous improvement processes
B. Documentation of key management practices
C. An exception management process
D. A change control process

Answer: C

Explanation:

An exception management process is a method for documenting and approving an exception to compliance with established IT governance policies, standards, and practices. An exception management process can accommodate the need for autonomy over technology choices by allowing a functional group to request and justify a deviation from the IT governance requirements, based on the business needs, risks, costs, and benefits. An exception management process can also help to ensure that the exceptions are reviewed and approved by the appropriate authorities, that the exceptions are monitored and reported, and that the exceptions are aligned with the IT strategy and objectives123. Reference: Exception Management Process Flow. IT/Information Security Exception Request Process. Strategies, Governance, Policies, Standards and Resources.

Question: 25

A board of directors wants to ensure the enterprise is responsive to changes in its environment that would directly impact critical business processes. Which of the following will BEST facilitate meeting this objective?

A. Scheduling frequent threat analyses
B. Monitoring key risk indicators (KRIs)
C. Regularly reviewing the enterprise risk appetite
D. Implementing a competitive intelligence tool

Answer: B

Explanation:

Key risk indicators (KRIs) are metrics that predict potential risks that can negatively impact businesses. They provide a way to quantify and monitor each risk. Think of them as change-related metrics that act as an early warning risk detection system to help companies effectively monitor, manage and mitigate risks1. By monitoring KRIs, the board of directors can ensure the enterprise is responsive to changes in its environment that would directly impact critical business processes, such as market fluctuations, customer preferences, regulatory compliance, operational efficiency, or cyber threats. Monitoring KRIs can help the board of directors to identify and assess the current and emerging risks, to evaluate the effectiveness and performance of the risk management strategies and controls, to communicate and report the risk status and issues, and to take timely and appropriate actions to prevent or reduce the impact of the risks234. Reference: How to Develop Key Risk Indicators (KRIs) to Fortify Your Business. ThePower of KRIs in Enterprise Risk Management (ERM). KRI (Key Risk Indicator): Understanding KRI and why is it important?. Key Risk Indicators (KRIs).

Question: 26

An enterprise has established a new department to oversee the life cycle of activities that support data management objectives. Which of the following should be done NEXT?

A. Develop a business continuity plan (BCP).
B. Assess the current data business model.
C. Review data privacy requirements.
D. Establish a RACI chart

Answer: D

Explanation:

A RACI chart is a tool that defines the roles and responsibilities of different stakeholders in a project or a process. RACI stands for Responsible, Accountable, Consulted, and Informed. A RACI chart can help to clarify who is responsible for performing the tasks, who is accountable for the outcomes, who is consulted for input or feedback, and who is informed of the progress or results. A RACI chart can help to improve communication, collaboration, and coordination among the stakeholders, as well as to avoid confusion, duplication, or

conflict of work12.

If an enterprise has established a new department to oversee the life cycle of activities that support data management objectives, the next step should be to establish a RACI chart for the data management process. This can help to define the roles and responsibilities of the new department and other existing departments or units that are involved in the data management process, such as IT, business, security, compliance, etc. A RACI chart can also help to align the data management process with the enterprise's strategy and goals, and to ensure that the data management objectives are met effectively and efficiently34. Reference: What is a RACI Chart? Definition & Example. How to Use a RACI Matrix: Everything You Need to Know. Data Management Process: Definition & Best Practices. Data Lifecycle Management: A 2023 Guide for Your Business.

Question: 27

Which of the following is the MOST important attribute of an information steward?

A. The information steward manages the systems that process the relevant data.
B. The information steward has expertise in managing data quality systems.
C. The information steward is closely aligned with the business function.
D. The information steward is part of the information architecture group.

Answer: C

Explanation:

An information steward is a person who is responsible for ensuring the quality, accuracy, consistency, and usability of the data in an organization. An information steward works with the business users and stakeholders to understand their data needs, requirements, and expectations, and to define and implement the data policies, standards, and rules that govern the data lifecycle. An information steward also monitors and reports on the data quality issues and trends, and initiates and coordinates the data improvement actions and projects12.

The most important attribute of an information steward is to be closely aligned with the business function, because this can help to ensure that the data supports the business goals and objectives, that the data meets the business expectations and requirements, that the data is relevant and useful for the business decisions and actions, and that the data is aligned with the business processes and workflows12.

The information steward does not necessarily manage the systems that process the relevant data, as this may be done by other IT roles, such as data engineers, data analysts, or data administrators. The information steward does not need to have expertise in managing data quality systems, as this may be a technical skill that can be acquired or supported by other IT roles or tools. The information steward does not need to be part of the information architecture group, as this may be a separate function that focuses on designing and maintaining the data structures, models, and standards12. Reference: Information Steward settings option descriptions - SAP Online Help. What is an Information Steward, and Why You Should Care?. 6 Key Responsibilities of the Invaluable Data Steward - Dun & Bradstreet.

Question: 28

From a governance perspective, which of the following roles is MOST important for an enterprise to keep in-house?

A. Information auditor
B. Information architect
C. Information steward

D. Information analyst

Answer: C

Explanation:

An information steward is a person who is responsible for ensuring the quality, accuracy, consistency, and usability of the data in an organization. An information steward works with the business users and stakeholders to understand their data needs, requirements, and expectations, and to define and implement the data policies, standards, and rules that govern the data lifecycle. An information steward also monitors and reports on the data quality issues and trends, and initiates and coordinates the data improvement actions and projects12.

From a governance perspective, the role of an information steward is most important for an enterprise to keep in-house, because it requires a close alignment with the business function, adeep knowledge of the data sources and systems, and a high level of trust and accountability. An information steward is the guardian of the business data, which is a valuable asset and a competitive advantage for any organization. Outsourcing the role of an information steward may pose significant risks to the data security, privacy, quality, and compliance12.

An information auditor is a person who performs independent and objective assessments of the data quality, integrity, and compliance in an organization. An information auditor evaluates the data governance policies, standards, and processes, as well as the data controls and safeguards. An information auditor also provides recommendations for improving the data management practices and mitigating the data risks3. An information auditor can be outsourced to provide an external and unbiased perspective on the data governance performance and issues.

An information architect is a person who designs and maintains the data structures, models, and standards in an organization. An information architect ensures that the data is organized, integrated, accessible, and consistent across different systems and platforms. An information architect also supports the data analysis, reporting, and visualization needs of the organization4. An information architect can be outsourced to leverage the expertise and experience of external consultants or vendors.

An information analyst is a person who collects, processes, analyzes, and interprets the data in an organization. An information analyst uses various tools and techniques to extract insights and value from the data. An information analyst also communicates and presents the data findings and recommendations to support decision making and problem solving in the organization. An information analyst can be outsourced to access specialized skills or technologies that may not be available in-house. Reference: What is Information Audit? Definition & Process. What is Information Architecture? Definition & Examples. What is an Information Steward? Definition & Role. 6 Key

Responsibilities of the Invaluable Data Steward - Dun & Bradstreet. [What is an Information Analyst? Definition & Skills].

Question: 29

An enterprise learns that a new privacy regulation was recently published to protect customers in the event of a breach involving personally identifiable information (PII). The IT risk management team's FIRST course of action should be to:

A. evaluate the risk appetite for the new regulation.
B. define the risk tolerance for the new regulation.
C. determine if the new regulation introduces new risk.
D. assign a risk owner for the new regulation.

Answer: C

Explanation:

A new privacy regulation is a legal requirement that aims to protect the rights and interests of customers in relation to their personal data, especially in the event of a breach involvingpersonally identifiable information (PII). A breach is an unauthorized or unlawful access, disclosure, alteration, or destruction of personal data that may compromise the confidentiality, integrity, or availability of the data1. A new privacy regulation may introduce new risk for an enterprise that collects, processes, stores, or transfers personal data of customers, such as legal, financial, reputational, or operational risk. Therefore, the IT risk management team's first course of action should be to determine if the new regulation introduces new risk for the enterprise, by assessing the scope, applicability, and impact of the regulation on the enterprise's data activities and practices. This can help the IT risk management team to identify and prioritize the gaps or issues that need to be addressed to comply with the regulation and to mitigate the potential risk23. Reference: What is a Data Breach? Definition & Examples. How to Manage Data Privacy Risks. Data Privacy Risk Management: A Guide for Businesses.

Question: 30

An enterprise has decided to utilize a cloud vendor for the first time to provide email as a service, eliminating in-house email capabilities. Which of the following IT strategic actions should be triggered by this decision?

A. Develop a data protection awareness education training program.
B. Monitor outgoing email traffic for malware.
C. Implement a data classification and storage management tool.
D. Update and communicate data storage and transmission policies.

Answer: D

Explanation:

Data storage and transmission policies are documents that define the rules and guidelines for how data is stored, accessed, shared, and transmitted within and outside an organization. Data storage and transmission policies can help to ensure the security, privacy, compliance, and quality of the data, as well as to prevent data loss, leakage, or breach12.

If an enterprise has decided to utilize a cloud vendor for the first time to provide email as a service, eliminating in-house email capabilities, one of the IT strategic actions that should be triggered by this decision is to update and communicate data storage and transmission policies. This is because using a cloud vendor for email as a service may introduce new risks and challenges for data storage and transmission, such as data sovereignty, data ownership, data encryption, data backup, data retention, data deletion, data access control, data audit, data breach notification, etc34. Therefore, it is important to update the data storage and transmission policies to reflect the changes in the email environment and the cloud vendor's responsibilities and obligations. It is also important to communicate the updated policies to all relevant stakeholders, such as employees, customers, partners, regulators, etc., to ensure their awareness and compliance12. Reference: Data Storage Policy: Definition & Best Practices. Data Transmission Policy: Definition & Best Practices. Cloud Email Security: Definition & Best Practices. Cloud Data Protection: Definition & Best Practices.

Question: 31

Which of the following components of a policy BEST enables the governance of enterprise IT?

A. Disciplinary actions
B. Regulatory requirements
C. Roles and responsibilities

D. Terms and definitions

Answer: C

Explanation:

A policy is a document that defines the rules and guidelines for how an organization conducts its activities and operations. A policy can help to ensure the compliance, consistency, and quality of the organization's performance and outcomes1. A policy typically consists of several components, such as purpose, scope, terms and definitions, roles and responsibilities, procedures, compliance, and review2.

From a governance perspective, one of the most important components of a policy is roles and responsibilities, because it clarifies who is accountable and responsible for implementing, enforcing, monitoring, and improving the policy. Roles and responsibilities can help to establish the authority, accountability, and communication among different stakeholders involved in the policy, such as the board of directors, senior management, business units, IT staff, customers, regulators, etc. Roles and responsibilities can also help to avoid confusion, duplication, or conflict of work among the stakeholders3 .

The governance of enterprise IT (GEIT) is the system by which the current and future use of IT is directed and controlled by an organization. GEIT aims to ensure that IT supports the organization's strategy and objectives, delivers value and benefits, manages risks and resources, and measures performance and outcomes. GEIT requires a clear definition of roles and responsibilities for the IT governance policies, processes, structures, and relationships. Some of the common roles and responsibilities involved in GEIT are:

The board of directors: provides strategic direction, oversight, and approval for IT governance
The senior management: provides leadership, support, and guidance for IT governance
The business units: provide input, feedback, and collaboration for IT governance
The IT function: provides execution, delivery, and improvement for IT governance
The audit function: provides assurance, evaluation, and recommendation for IT governance
The external stakeholders: provide requirements, expectations, and compliance for IT governance Reference: What is a Policy? Definition & Examples. Policy Components: Definition & Examples. Roles & Responsibilities in Policy Development. [Policy Development: Roles & Responsibilities]. [What is IT Governance? Definition & Frameworks]. [IT Governance Roles & Responsibilities]. [Roles & Responsibilities in IT Governance].

Question: 32

An enterprise has made the strategic decision to reduce operating costs for the next year and is taking advantage of cost reductions offered by an external cloud service provider. Which of the following should be the IT steering committee's PRIMARY concern?

A. Revising the business $ balanced store card
B. Updating the business risk profile
C. Changing the IT steering committee charter
D. Calculating the cost of the current solution

Answer: B

Explanation:

A business risk profile is a document that identifies and evaluates the potential risks that can affect the performance, objectives, and strategy of an organization. A business risk profile can help to prioritize and mitigate the risks, as well as to align the risk management activities with the business goals and needs12.

If an enterprise has made the strategic decision to reduce operating costs for the next year and is taking

advantage of cost reductions offered by an external cloud service provider, the IT steering committee's primary concern should be updating the business risk profile. This is because using an external cloud service provider may introduce new or increased risks for the enterprise, such as security, privacy, compliance, availability, performance, or vendor lock-in risks3 . Updating the business risk profile can help the IT steering committee to assess the impact and likelihood of these risks, to evaluate the effectiveness and adequacy of the existing controls and safeguards, to identify and implement any additional measures or actions to address the gaps or issues, and to monitor and report the risk status and outcomes12. Reference: Business Risk Profile: Definition & Examples. How to Create a Business Risk Profile. A risk assessment model for selecting cloud service providers. Cloud Computing Security for Cloud Service Providers.

Question: 33

An IT investment review board wants to ensure that IT will be able to support business initiatives. Each initiative is comprised of several interrelated IT projects. Which of the following would help ensure that the initiatives meet their goals?

A. Review of project management methodology
B. Review of the business case for each initiative
C. Establishment of portfolio management
D. Verification of initiatives against the architecture

Answer: C

Explanation:

Portfolio management is the process of selecting, prioritizing, and managing a collection of projects, programs, and initiatives that align with the strategic goals and objectives of an organization.
Portfolio management can help to ensure that the IT initiatives meet their goals, by providing a holistic and integrated view of the IT investments, resources, and outcomes. Portfolio management can also help to optimize the value and benefits of the IT initiatives, by balancing the risks, costs, and dependencies among them. Portfolio management can also help to monitor and control the performance and progress of the IT initiatives, by using metrics, indicators, and reports123. Reference: What is Portfolio Management? Definition & Examples. A Guide to IT Portfolio Management | Adobe Workfront. IT Portfolio Management: Importance, How-To Steps and Tips.

Question: 34

It has been discovered that multiple business units across an enterprise are using duplicate IT applications and services to fulfill their individual needs. Which of the following would be MOST helpful to address this concern?

A. Enterprise architecture (EA)
B. Enterprise risk framework
C. IT service management
D. IT project roadmap

Answer: A

Explanation:

Enterprise architecture (EA) is a discipline that defines and organizes the components, relationships, principles, and standards of an organization's IT environment. EA can help to align IT with business strategy and objectives, optimize IT performance and value, and manage IT complexity and change12.
One of the benefits of EA is that it can help to address the concern of duplicate IT applications and services

across an enterprise. EA can help to identify and eliminate the redundancies, inconsistencies, and inefficiencies in the IT landscape, by providing a holistic and integrated view of the current and future state of IT. EA can also help to rationalize and consolidate the IT applications and services, by establishing a common framework, taxonomy, and governance for IT decision making. EA can also help to improve the integration and interoperability of IT applications and services, by defining the interfaces, protocols, and standards for data exchange123.

Some examples of how EA can help to address the concern of duplicate IT applications and services are:

EA can help to conduct an inventory and assessment of the existing IT applications and services, to determine their purpose, scope, functionality, quality, cost, and value. EA can also help to compare and contrast the IT applications and services across different business units, to identify the overlaps, gaps, or conflicts among them4.

EA can help to define and prioritize the business needs and requirements for IT applications and services, to ensure that they support the business goals and processes. EA can also help to evaluate and select the best IT solutions for each business need, based on criteria such as feasibility, suitability, scalability, security, compliance, etc5.

EA can help to design and implement a target IT architecture that eliminates or minimizes the duplicate IT applications and services, by using approaches such as application portfolio management (APM), service-oriented architecture (SOA), or cloud computing. EA can also help to plan and execute a migration strategy that ensures a smooth transition from the current to the target state .

EA can help to monitor and control the IT applications and services, by using metrics, indicators, and reports to measure their performance, availability, reliability, quality, and value. EA can also help to review and update the IT applications and services regularly, by using feedback mechanisms and continuous improvement practices .

Reference:

What is Enterprise Architecture? Definition & Frameworks. Enterprise Architecture: Definition & Best Practices. How Enterprise Architecture Can Help You Eliminate Technical Debt. Application Inventory: Definition & Best Practices. Business Requirements: Definition & Best Practices. [Application Portfolio Management: Definition & Best Practices]. [Service-Oriented Architecture: Definition & Benefits]. [IT Performance Management: Definition & Best Practices]. [Continuous Improvement: Definition & Best Practices].

Question: 35

Results of an enterprise's customer survey indicate customers prefer using mobile applications. However, this same survey shows the enterprise's mobile applications are considered inferior compared to legacy browser-based applications. Which of the following should be the FIRST step in creating an effective long-term mobile application strategy?

A. Establish service level agreements (SLAs) with the development team.
B. Identify key risks and mitigation strategies for mobile applications.
C. Implement key performance indicators (KPIs) that include application quality.
D. Identify business requirements concerning mobile applications.

Answer: D

Explanation:

The first step in creating an effective long-term mobile application strategy is to identify the business requirements concerning mobile applications. Business requirements are the needs, expectations, and objectives of the business stakeholders and customers for a product or service. Business requirements can help to define the scope, purpose, value, and quality of the mobile applications, as well as to align them with the business strategy and goals12.

By identifying the business requirements concerning mobile applications, the enterprise can understand what the customers want and need from the mobile applications, what problems or pain points they are facing with the current applications, what features or functions they are looking for or missing, what benefits or outcomes they are expecting or measuring, and what preferences or feedback they have for improving the mobile applications12.

Identifying the business requirements concerning mobile applications can also help the enterprise to prioritize and plan the development, testing, and deployment of the mobile applications, by using criteria such as feasibility, suitability, scalability, security, compliance, etc. Identifying the business requirements concerning mobile applications can also help the enterprise to monitor and evaluate the performance and satisfaction of the mobile applications, by using metrics, indicators, and reports12.

Therefore, identifying the business requirements concerning mobile applications is the first step in creating an effective long-term mobile application strategy. This can help the enterprise to deliver mobile applications that meet or exceed the customer expectations and requirements, and that are superior to the legacy browser-based applications. Reference: Business Requirements: Definition & Best Practices. How to Write a Business Requirements Document: A Comprehensive Guide.

Question: 36

Which of the following is the GREATEST impact to an enterprise that has ineffective information architecture?

A. Poor desktop service delivery
B. Data retention
C. Redundant systems
D. Poor business decisions

Answer: D

Explanation:

Information architecture (IA) is the practice of structuring and presenting the parts of something — whether that's a website, mobile app, blog post, book, or brick-and-mortar store — to users so that it's easy to understand. IA can help users find information and complete tasks1.

An enterprise that has ineffective information architecture may suffer from poor business decisions, because it may not be able to access, analyze, or use the data and information that are relevant, accurate, consistent, and timely for decision making. Poor business decisions can lead to negative consequences, such as losing customers, market share, revenue, or competitive advantage, or facing legal, financial, reputational, or operational risks23.

Some examples of how ineffective information architecture can impact business decisions are:

If the enterprise's website has a confusing or inconsistent navigation system, users may not be able to find the information they need or want, such as product details, prices, reviews, or contactinformation. This can result in lower customer satisfaction, engagement, conversion, and retention14.

If the enterprise's data is stored in multiple systems or platforms that are not integrated or interoperable, users may not be able to access or share the data across different departments or functions. This can result in data silos, duplication, inconsistency, or incompleteness25.

If the enterprise's data is not labeled or categorized properly, users may not be able to search or filter the data effectively. This can result in data overload, irrelevance, or obscurity25.

If the enterprise's data is not governed or managed properly, users may not be able to trust or verify the data quality or integrity. This can result in data errors, inaccuracies, or biases25.

Therefore, an enterprise that has ineffective information architecture may have poor business decisions as its

greatest impact. Reference: Information Architecture Basics | Usability.gov. The Importance of Information Architecture to UX Design. How Enterprise Architecture Can Help You Eliminate Technical Debt. What Is Information Architecture & Why Does It Matter? - HubSpot Blog. Why Do We Need Information Architecture - Architecture.

Question: 37

Of the following, who should be responsible for ensuring the regular review of quality management performance against defined quality metrics?

A. Process owners
B. Risk management team
C. Internal auditors
D. Executive management

Answer: A

Explanation:

Process owners are responsible for ensuring the regular review of quality management performance against defined quality metrics, as they are accountable for the design, implementation and improvement of the processes they own. Risk management team, internal auditors and executive management have other roles and responsibilities in relation to quality management, such as providing assurance, oversight and direction. Reference: : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.2: IT Investment Management, Subsection 3.2.4: IT Investment Management Process, Page 104 : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.4: Quality Management, Subsection 3.4.1: Quality Management Overview, Page 120

Question: 38

An enterprise experiencing issues with data protection and least privilege is implementing enterprise-wide data encryption in response. Which of the following is the BEST approach to ensure all business units work toward remediating these issues?

A. Develop key performance indicators (KPIs) to measure enterprise adoption.
B. Integrate data encryption requirements into existing and planned projects.
C. Assign owners for data governance initiatives.
D. Mandate the creation of a data governance framework.

Answer: D

Explanation:

A data governance framework is a set of policies, standards, roles, and processes that define how data is collected, stored, accessed, and used within an enterprise. A data governance framework can help address data protection and least privilege issues by establishing clear rules and responsibilities for data owners, custodians, and users. A data governance framework can also enable data encryption as a key control to protect sensitive data from unauthorized access or disclosure. Therefore, mandating the creation of a data governance framework is the best approach to ensure all business units work toward remediating these issues. Reference: : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.2: IT Risk Management Process, Page 156 : CGEIT Review Manual (Digital Version), Chapter 5: Resource Optimization, Section 5.2: Information Resource Management, Subsection 5.2.1: Information Resource Management Overview, Page 183 : A Guide to Selecting and Adopting a Privacy Framework1

Question: 39

Senior management wants to promote investment in IT, but is uncertain that associated risks are being properly identified. The BEST way to address this concern is to:

A. engage an external consultant to develop risk scenarios.
B. appoint an IT representative to the business risk committee.
C. assign an IT cost controller to the finance department.
D. ensure business cases are developed by IT.

Answer: B

Explanation:

Appointing an IT representative to the business risk committee is the best way to address senior management's concern about IT investment risks, as it would ensure that IT risks are properly identified, assessed, and communicated to the business stakeholders. The IT representative would also be able to align IT risk management with the enterprise's risk appetite and strategy, and provide input and feedback on the IT investment decisions. The other options are not as effective, as they do not involve direct collaboration and communication between IT and business on risk matters. Reference: : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.1: IT Risk Management Overview, Page 153 : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.2: IT Risk Management Process, Page 156 :CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.5: Roles and Responsibilities for IT Risk Management, Page 161

Question: 40

Which of the following represents the GREATEST challenge to implementing IT governance?

A. Determining the best practice to follow
B. Planning the project itself
C. Developing a business case
D. Applying behavioral change management

Answer: D

Explanation:

Applying behavioral change management is the greatest challenge to implementing IT governance, as it involves changing the culture, mindset, and behavior of the people who are affected by or involved in IT governance. IT governance is not just a technical or procedural issue, but also a human and organizational one. Therefore, it requires effective communication, education, motivation, and leadership to ensure that the stakeholders understand, accept, and support the IT governance objectives, principles, and practices. The other options are not as challenging, as they can be addressed by following established methods, frameworks, and standards for IT governance. Reference: : CGEIT Review Manual (Digital Version), Chapter 1: Governance of Enterprise IT, Section 1.2: IT Governance Frameworks and Standards, Subsection 1.2.1: IT Governance Frameworks and Standards Overview, Page 17 : CGEIT Review Manual (Digital Version), Chapter 1: Governance of Enterprise IT, Section 1.4: Implementing and Maintaining an IT Governance Framework, Subsection 1.4.2: Implementing an IT Governance Framework, Page 29 : CGEIT Preparation Tips and the Timelessness of Good Governance1

Question: 41

Which of the following is the BEST method for making a strategic decision to invest in cloud services?

A. Prepare a business case.
B. Prepare a request for information (RFI),
C. Benchmarking.
D. Define a balanced scorecard.

Answer: A

Explanation:

A business case is the best method for making a strategic decision to invest in cloud services, as it provides a structured and comprehensive analysis of the costs, benefits, risks, and value proposition of the proposed investment. A business case can help justify the need for cloudservices, compare different options and alternatives, and align the investment with the enterprise's strategy and objectives. A request for information (RFI) is a document that solicits information from potential vendors or suppliers, but it does not provide a decision-making framework. Benchmarking is a process of comparing the performance or practices of an enterprise with those of others, but it does not evaluate the feasibility or desirability of cloud services. A balanced scorecard is a tool that measures and monitors the performance of an enterprise or a business unit against strategic goals and objectives, but it does not assess the viability or suitability of cloud services. Reference: : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.2: IT Investment Management, Subsection 3.2.1: IT Investment Management Overview, Page 97 : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.2: IT Investment Management, Subsection 3.2.4: IT Investment Management Process, Page 104 : How to Write a Business Case: Template & Examples1

Question: 42

An enterprise is developing several consumer-based services using emerging technologies involving sensitive personal data. The CIO is under pressure to ensure the enterprise is first to market, but security scan results have not been adequately addressed. Reviewing which of the following will enable the CIO to make the BEST decision for the customers?

A. Acceptable use policy
B. Risk register
C. Ethics standards
D. Change management policy

Answer: B

Explanation:

A risk register is a tool that records and tracks the risks associated with a project or an activity, such as developing consumer-based services using emerging technologies involving sensitive personal data. A risk register typically includes information such as the risk description, category, impact, probability, status, response strategy, and owner. Reviewing the risk register will enable the CIO to make the best decision for the customers, as it will help them to identify, assess, and prioritize the risks that may affect the security, privacy, and quality of the services, and to determine the appropriate actions to mitigate or avoid them. The other options are not as relevant, as they do not provide specific information about the risks involved in the project or activity. Reference: : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.2: IT Risk Management Process, Page 156 : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.3: IT Risk Management Techniques and Tools, Page 158 : Capability Maturity Model and Risk Register Integration1

Question: 43

An organization's board of directors has questioned the value provided by IT key performance indicators (KPIs). Which of the following is the BEST way to determine whether the KPIs adequately support organizational objectives?

A. Define a strategy for IT measurement.
B. Define policies and procedures around current KPIs.
C. Review the KPIs with key business executives.
D. Work directly with the CEO to identify what measures should be used.

Answer: A

Explanation:

Defining a strategy for IT measurement is the best way to determine whether the KPIs adequately support organizational objectives, as it would help to establish a clear vision, scope, purpose, and alignment of the IT measurement activities. A strategy for IT measurement would also help to identify the relevant stakeholders, roles, responsibilities, and expectations for the IT measurement process, and to define the criteria, methods, and tools for selecting, collecting, analyzing, and reporting the KPIs. The other options are not as effective, as they do not address the root cause of the board's question, which is the lack of a coherent and consistent approach to IT measurement. Reference: : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.3: Performance Measurement and Reporting, Subsection 3.3.1: Performance Measurement and Reporting Overview, Page 112 : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.3: Performance Measurement and Reporting, Subsection 3.3.2: Performance Measurement and Reporting Process, Page 113 : The Value of IT Governance

Question: 44

Which of the following is PRIMARILY achieved through performance measurement?

A. Process improvement
B. Transparency
C. Cost efficiency
D. Benefit realization

Answer: B

Explanation:

Transparency is primarily achieved through performance measurement, as it involves providing clear, accurate, and timely information about the performance of IT processes, services, and projects to the relevant stakeholders. Performance measurement can help to increase the visibility, accountability, and trustworthiness of IT activities and outcomes, and to enable informed decisionmaking and feedback. The other options are not as primary, as they are more related to the results or consequences of performance measurement, rather than the purpose orintention of it. Reference: : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.3: Performance Measurement and Reporting, Subsection 3.3.1: Performance Measurement and Reporting Overview, Page 112 : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.3: Performance Measurement and Reporting, Subsection 3.3.2: Performance Measurement and Reporting Process, Page 113 : Performance Measurement Metrics for IT Governance1

Question: 45

A large retail chain realizes that while there has not been any loss of data, IT security has not been a priority and should become a key goal for the enterprise. What should be the FIRST high-level initiative for a newly created IT strategy committee in order to support this business goal?

A. Identifying gaps in information asset protection
B. Defining data archiving and retrieval policies
C. Recruiting and training qualified IT security staff
D. Modernizing internal IT security practices

Answer: A

Explanation:

Identifying gaps in information asset protection should be the first high-level initiative for a newly created IT strategy committee in order to support the business goal of making IT security a priority. This initiative would help to assess the current state of IT security, identify the risks and vulnerabilities that may compromise the confidentiality, integrity, and availability of information assets, and determine the actions and resources needed to address them. The other options are not as high-level, as they are more related to the implementation or execution of IT security, rather than the planning or direction of it. Reference: : CGEIT Review Manual (Digital Version), Chapter 1: Governance of Enterprise IT, Section 1.3: Strategic Management, Subsection 1.3.2: Strategic Management Process, Page 23 : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.2: IT Risk Management Process, Page 156 : CGEIT Review Manual (Digital Version), Chapter 5: Resource Optimization, Section 5.3: Security Resource Management, Subsection 5.3.1: Security Resource Management Overview, Page 192 : What is CGEIT? A certification for seasoned IT governance professionals1

Question: 46

Risk management strategies are PRIMARILY adopted to:
A. avoid risks for business and IT assets.
B. take necessary precautions for claims and losses.
C. achieve acceptable residual risk levels.
D. achieve compliance with legal requirements.

Answer: C

Explanation:

Risk management strategies are primarily adopted to achieve acceptable residual risk levels, which are the levels of risk that remain after applying risk response measures. Risk management strategies are the approaches or methods that an organization uses to identify, assess, and treat its IT-related risks. Risk management strategies can vary depending on the organization's risk appetite, tolerance, and capacity, as well as the nature and impact of the risks. Some common risk management strategies are: avoid, reduce, transfer, share, or accept. The other options are not as primary, as they are more related to the outcomes or objectives of risk management strategies, rather than the purpose or intention of them. Reference: : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.1: IT Risk Management Overview, Page 153 : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.2: IT Risk Management Process, Page 156 : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.3: IT Risk Management Techniques and Tools, Page 158 : Proactive IT Risk Management in an Era of Emerging Technologies1

Question: 47

An enterprise made a significant change to its business operating model that resulted in a new strategic direction. Which of the following should be reviewed FIRST to ensure IT congruence with the new business strategy?

A. IT risk appetite
B. Enterprise project management framework
C. IT investment portfolio
D. Information systems architecture

Answer: C

Explanation:

An IT investment portfolio is a collection of IT projects, programs, and services that are funded and implemented by an enterprise to achieve its strategic and operational objectives. An IT investment portfolio should be reviewed first to ensure IT congruence with the new business strategy, as it would help to align the IT investments with the business goals, priorities, and needs. A review of the IT investment portfolio would also help to identify and evaluate the current and planned IT initiatives, assess their costs, benefits, risks, and value, and optimize the allocation of IT resources and capabilities. The other options are not as relevant, as they are more related to the execution or delivery of IT activities, rather than the planning or direction of them.
Reference: : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.2: IT Investment Management, Subsection 3.2.1: IT Investment ManagementOverview, Page 97 : CGEIT Review Manual (Digital Version), Chapter 3: Benefits Realization, Section 3.2: IT Investment Management, Subsection 3.2.4: IT Investment Management Process, Page 104 : The Power of IT Investment Risk Quantification and Visualization: IT Portfolio Management

Question: 48

A chief technology officer (CTO) wants to ensure IT governance practices adequately address risk management specific to mobile applications. To create the appropriate risk policies for IT, it is MOST important for the CTO to:

A. understand the enterprise's risk tolerance.
B. create an IT risk scorecard.
C. map the business goals to IT risk processes.
D. identify the mobile technical requirements.

Answer: A

Explanation:

Understanding the enterprise’s risk tolerance is the most important step for the CTO to create the appropriate risk policies for IT, as it would help to define the acceptable level of risk exposure and the risk appetite for mobile applications. Risk tolerance is the degree of uncertainty that an enterprise is willing to accept in pursuit of its objectives, and it reflects the enterprise’s culture, strategy, and stakeholder expectations. Risk policies for IT should be aligned with the enterprise’s risk tolerance, as well as its mission, vision, and goals. The other options are not as important, as they are more related to the implementation or measurement of risk management, rather than the establishment of risk policies. Reference: : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.1: IT Risk Management Overview, Page 153 : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.2: IT Risk Management Process, Page 156 : Proactive IT Risk Management in an Era of Emerging Technologies

Question: 49

A large financial institution is considering outsourcing customer call center operations which will allow the chosen vendor to access systems from offshore locations. Which of the following represents the GREATEST risk?

A. Inconsistent customer service and reporting
B. Loss of data confidentiality
C. Lack of network availability
D. Inadequate business continuity planning

Answer: B

Explanation:

Loss of data confidentiality represents the greatest risk for a large financial institution that is considering outsourcing customer call center operations, as it would expose sensitive customer and business information to unauthorized access, disclosure, or misuse by the chosen vendor or other third parties. Data confidentiality is especially important for financial institutions, as they deal with personal, financial, and transactional data that are subject to strict regulatory and legal requirements, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). A breach of data confidentiality could result in reputational damage, customer dissatisfaction, legal liability, and financial loss for the financial institution. The other options are not as great, as they are more related to the operational or performance aspects of outsourcing, rather than the security or compliance aspects of it. Reference: : CGEIT Review Manual (Digital Version), Chapter 4: Risk Optimization, Section 4.3: IT Risk Management, Subsection 4.3.1: IT Risk Management Overview, Page 153 : CGEIT Review Manual (Digital Version), Chapter 5: Resource Optimization, Section 5.3: Security Resource Management, Subsection 5.3.1: Security Resource Management Overview, Page 192 : Offshore bank call centers face risks around privacy, resilience amid COVID-191 : Call Center Outsourcing Risks and How to Mitigate Them

Question: 50

An IT director is negotiating a contract with a vendor for application management services. There is concern by other departments that the outsourced services may not be delivered successfully. Which of the following is the BEST way for the IT director to address this concern?

A. Implement a communication management plan.
B. Develop a comprehensive vendor management plan.
C. Review the IT service risk management plan.
D. Establish a policy on operational level agreements with vendors.

Answer: B

Explanation:

The best way for the IT director to address the concern of other departments about the outsourced services is to develop a comprehensive vendor management plan. A vendor management plan is a document that details how the IT director and the vendor will work together to achieve the objectives and expectations of the contract. A vendor management plan can include the following elements1:

Scope of work: This defines the services, deliverables, and outcomes that the vendor will provide, as well as the roles and responsibilities of both parties.

Service level agreements (SLAs): These specify the performance standards, metrics, and targets that the vendor will adhere to, as well as the penalties or rewards for meeting or exceeding them. Operational level agreements (OLAs): These describe the internal processes and procedures that the IT director and the vendor will follow to support the SLAs, such as communication, escalation, reporting, and issue resolution.

Risk management: This identifies and assesses the potential risks that may affect the delivery of the outsourced services, such as security, compliance, quality, or continuity, and defines the mitigation strategies and contingency plans to address them.

Governance: This establishes the governance structure and mechanisms that will oversee and monitor the vendor relationship, such as steering committees, audits, reviews, and feedback. A comprehensive vendor management plan can help to ensure that the outsourced services are delivered successfully by providing clarity, transparency, accountability, and alignment between the IT director and the vendor. It can also help to address the concerns of other departments by demonstrating that the IT director has taken adequate measures to manage and control the vendor performance and risk. Additionally, a vendor management plan can help to foster a collaborative and trusting relationship between the IT director and the vendor, which can lead to improved service quality, efficiency, and innovation.

1: 3 Steps to Improve Strategic Vendor Management

Question: 51

Which of the following is the BEST IT architecture concept to ensure consistency, interoperability, and agility for infrastructure capabilities?

A. Establishment of an IT steering committee
B. Standards-based reference architecture and design specifications
C. Establishment of standard vendor and technology designations
D. Design of policies and procedures

Answer: B

Explanation:

Standards-based reference architecture and design specifications. A reference architecture is a set of principles, patterns, standards, and best practices that guide the design and implementation of IT solutions. A design specification is a detailed document that describes the technical requirements, features, and functionalities of an IT solution. By using standards-based reference architecture and design specifications, an enterprise can ensure that its IT infrastructure is aligned with its business needs and goals, and that it can support the integration, compatibility, and scalability of its IT systems and services. Some examples of standards-based reference architectures are: The Open Group Architecture Framework (TOGAF) 1, The Federal Enterprise Architecture Framework (FEAF) 2, and The Cloud Computing Reference Architecture (CCRA) 3.

Question: 52

A company is considering selling products online, and the CIO has been asked to advise the board of directors of potential problems with this strategy. Which of the following is the ClO's BEST course of action?

A. Review the security framework.
B. Conduct a return on investment (ROI) analysis.
C. Review the enterprise architecture (EA).
D. Perform a risk assessment.

Answer: D

Explanation:

A risk assessment is a process of identifying, analyzing, and evaluating the potential risks that may affect the achievement of an objective, such as selling products online. A risk assessment can help the CIO to advise the board of directors of the possible threats, vulnerabilities, and impacts that may arise from the online sales strategy, such as cyberattacks, data breaches, fraud, legal compliance, customer satisfaction, and reputation. A risk assessment can also help the CIO to recommend the appropriate risk response measures, such as avoiding, reducing, transferring, or accepting the risks. The other options are not as effective, as they do not address the

potential problems with the online sales strategy in a holistic and systematic way. Reviewing the security framework may help to ensure that the online sales platform is secure and resilient, but it does not consider other aspects of risk, such as business, legal, or operational. Conducting a return on investment (ROI) analysis may help to estimate the financial benefits and costs of the online sales strategy, but it does not account for the uncertainties and variabilities of risk. Reviewing the enterprise architecture (EA) may help to align the online sales strategy with the business goals and capabilities, but it does not assess the likelihood and consequences of risk.

Question: 53

In a large enterprise, which of the following is the MOST effective way to understand the business activities associated with the enterprise's information architecture?

A. Reviewing IT design with business process managers
B. Reviewing business strategy with senior management
C. Mapping business processes within a framework
D. Aligning business objectives to organizational strategy

Answer: C

Explanation:

Mapping business processes within a framework is the most effective way to understand the business activities associated with the enterprise's information architecture, as it provides a clear and comprehensive view of how information flows and supports the businessobjectives. Reference:= CGEIT Exam Content Outline, Domain 1, Subtopic C: Information Governance, Task 1: Define and implement information governance processes to ensure alignment with enterprise goals and objectives.

Question: 54

A board of directors is concerned that a major IT implementation has the potential to significantly disrupt enterprise operations. Which of the following would be MOST helpful in identifying the extent of the potential impact of the disruption?

A. An analysis of the current enterprise risk appetite
B. An earned value analysis (EVA) of the implementation
C. A risk assessment of the implementation
D. A review of lessons learned from previous implementations

Answer: C

Explanation:

A risk assessment of the implementation would be most helpful in identifying the extent of the potential impact of the disruption, as it would evaluate the likelihood and consequences of various scenarios that could affect the enterprise operations. A risk assessment would also help to identify and prioritize the mitigation strategies and contingency plans for the implementation. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 1: Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework1.

Question: 55

Which of the following is the MOST comprehensive method to report on overall IT performance to the board of directors?

A. Balanced scorecard

B. Net present value (NPV)
C. Performance-based payments
D. Return on investment (ROI)

Answer: A

Explanation:

A balanced scorecard is the most comprehensive method to report on overall IT performance to the board of directors, as it provides a holistic view of the IT value proposition, covering four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard helps to align IT goals and objectives with the enterprise strategy, measure and monitor IT performance, and communicate IT value to the board and other stakeholders123. Reference := CGEIT Exam Content Outline, Domain 3, Subtopic B:Performance Measurement and Optimization, Task 1: Establish and monitor IT performance measurement systems to evaluate the extent to which IT delivers on its strategic objectives and desired outcomes.

Question: 56

A CIO has been asked to modify an organization's IT performance measurement system to reflect recent changes in technology, including the movement of some data processing to a cloud solution. Which of the following is the PRIMARY consideration when designing such a measurement system?

A. Ensuring that cost of measurement and reporting is minimized
B. Ensuring the measurement system maps to the enterprise architecture (EA)
C. Adequately defining the scope of services moved to the cloud
D. Correctly understanding stakeholder needs for IT-related measurement

Answer: D

Explanation:

Correctly understanding stakeholder needs for IT-related measurement is the primary consideration when designing such a measurement system, as it ensures that the system is relevant, useful, and aligned with the enterprise goals and objectives. Stakeholder needs can be identified and prioritized using various techniques, such as the goals cascade, which links stakeholder needs to enterprise goals, IT-related goals, and enabler goals1. The measurement system should also be adaptable to changes in technology and business environment, such as the movement of some data processing to a cloud solution. Reference := CGEIT Exam Content Outline, Domain 3, Subtopic B: Performance Measurement and Optimization, Task 1: Establish and monitor IT performance measurement systems to evaluate the extent to which IT delivers on its strategic objectives and desired outcomes.

Question: 57

Which of the following MOST effectively demonstrates operational readiness to address information security risk issues?

A. Executive management has announced an information security risk initiative.
B. IT management has communicated the need for information security risk management to the business.
C. A policy has been communicated stating enterprise commitment and readiness to address information security risk.
D. Procedures have been established for assessing and mitigating information security risks.

Answer: D

Explanation:

Procedures have been established for assessing and mitigating information security risks is the most effective way to demonstrate operational readiness to address information security risk issues, as it shows that the enterprise has a systematic and consistent approach to identify, analyze, treat, and monitor information security risks. Procedures also provide guidance and direction for the staff involved in information security risk management activities12. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 1: Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework.

Question: 58

An enterprise's CIO requires all IT processes within the enterprise to be clearly defined. Which of the following would be the MOST immediate outcome?

A. Performance
B. Repeatability
C. Scalability
D. Optimization

Answer: B

Explanation:

Repeatability is the most immediate outcome of defining all IT processes within the enterprise, as it ensures that the processes can be performed consistently and reliably by different people or teams, following the same steps and procedures. Repeatability also enables the measurement and improvement of IT processes over time12. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 2: Ensure that IT governance is aligned with the enterprise governance framework and is integrated into the enterprise governance approach.

Question: 59

Best practice states that IT governance MUST:

A. enforce consistent policy across the enterprise.
B. be applied in the same manner throughout the enterprise.
C. apply consistent target levels of maturity to processes.
D. be a component of enterprise governance.

Answer: D

Explanation:

IT governance must be a component of enterprise governance, as it ensures that IT supports and enables the achievement of the enterprise goals and objectives. IT governance is the responsibility of the board of directors and executive management, and it is an integral part of enterprise governance123. IT governance also aligns IT with the enterprise strategy, deliversvalue from IT investments, manages IT risks and resources, and measures IT performance3. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 1: Ensure the definition, establishment, and management of a framework for the governance of enterprise IT in alignment with the mission, vision and values of the enterprise.

Question: 60

The MOST important aspect of an IT governance framework to ensure that IT supports repeatable business processes is:

A. earned value management.

B. quality management,
C. resource management.
D. risk management

Answer: B

Explanation:

Quality management is the most important aspect of an IT governance framework to ensure that IT supports repeatable business processes, as it involves defining, implementing, and monitoring quality standards, policies, and procedures for IT products and services. Quality management also ensures that IT processes are aligned with the enterprise requirements, objectives, and expectations, and that they deliver consistent and reliable outcomes12. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic C: Technology Governance, Task 2: Ensure that IT processes are defined, implemented, monitored and continually improved in alignment with the enterprise governance framework.

Question: 61

A new CIO has been charged with updating the IT governance structure. Which of the following is the MOST important consideration to effectively influence organizational and process change?

A. Obtaining guidance from consultants
B. Aligning IT services to business processes
C. Redefining the IT risk appetite
D. Ensuring the commitment of stakeholders

Answer: D

Explanation:

Ensuring the commitment of stakeholders is the most important consideration to effectively influence organizational and process change, as it involves engaging and communicating with the key parties who have an interest or influence in the IT governance structure. Stakeholder commitment can help to overcome resistance, gain support, and ensure alignment and collaboration among the enterprise units1. Stakeholder commitment can also facilitate theadoption and implementation of the IT governance framework, policies, and standards . Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 3: Ensure that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Question: 62

The PRIMARY benefit of integrating IT resource planning into enterprise strategic planning is that it enables the enterprise to:

A. allocate resources efficiently to achieve desired goals.
B. adjust business goals depending upon resource availability.
C. prioritize resource allocation based on sourcing strategy.
D. develop tactical plans to achieve resource optimization.

Answer: A

Explanation:

Integrating IT resource planning into enterprise strategic planning enables the enterprise to allocate resources efficiently to achieve desired goals, as it ensures that IT resources are aligned with the enterprise vision,

mission, and objectives. IT resource planning also helps to identify and prioritize the IT needs and demands of the enterprise, and to allocate the appropriate resources (such as people, processes, technology, and information) to meet them123. Reference := CGEIT Exam Content Outline, Domain 2, Subtopic A: IT Resource Planning, Task 1: Ensure that IT resource planning is aligned with the enterprise strategic planning process.

Question: 63

An enterprise is implementing a new IT governance program. Which of the following is the BEST way to increase the likelihood of its success?

A. The IT steering committee approves the implementation efforts.
B. The CIO communicates why IT governance is important to the enterprise.
C. Implementation follows an IT audit recommendation.
D. The CIO issues a mandate for adherence to the program.

Answer: B

Explanation:

The CIO communicating why IT governance is important to the enterprise is the best way to increase the likelihood of its success, as it helps to create awareness, understanding, and buy-in from the stakeholders and staff involved in the IT governance program. The CIO can also communicate the benefits, objectives, and expectations of the IT governance program, and how italigns with the enterprise strategy and vision123. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 3: Ensure that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Question: 64

Which of the following is the PRIMARY element in sustaining an effective governance framework?

A. Identification of optimal business resources
B. Establishment of a performance metric system
C. Ranking of critical business risks
D. Assurance of the execution of business controls

Answer: D

Explanation:

Assurance of the execution of business controls is the primary element in sustaining an effective governance framework, as it ensures that the IT governance processes and activities are performed in accordance with the established policies, standards, and procedures. Assurance also provides feedback and monitoring on the performance, compliance, and outcomes of the IT governance framework, and identifies areas for improvement and optimization12. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 5: Ensure that assurance processes are established to provide confidence that the IT governance framework is designed and operating effectively.

Question: 65

A global financial enterprise has been experiencing a substantial number of information security incidents that have directly affected its business reputation. Which of the following should be the IT governance board's FIRST course of action?

A. Require revisions to how security incidents are managed by the IT department.

B. Request an IT security assessment to identify the main security gaps.
C. Execute an IT maturity assessment of the security process.
D. Mandate an update to the enterprise's IT security policy.

Answer: B

Explanation:

Requesting an IT security assessment to identify the main security gaps is the IT governance board's first course of action, as it helps to understand the root causes and the extent of the information security incidents that have affected the enterprise's business reputation. An IT security assessment can also provide recommendations and best practices for improving thesecurity posture and reducing the risks of future incidents12. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 1: Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM)
framework.

Question: 66

An enterprise has had the same IT governance framework in place for several years. Currently, large and small capital projects go through the same architectural governance reviews. Despite repeated requests to streamline the review process for small capital projects, business units have received no response from IT. The business units have recently escalated this issue to the newly appointed GO. Which of the following should be done FIRST to begin addressing business needs?

A. Create a central repository for the business to submit requests.
B. Explain the importance of the IT governance framework.
C. Assess the impact of the proposed change.
D. Assign a project team to implement necessary changes.

Answer: C

Explanation:

Assessing the impact of the proposed change is the first step to begin addressing business needs, as it helps to understand the current state of the IT governance framework, the gaps and issues that need to be resolved, and the potential benefits and risks of the change. An impact assessment can also provide a basis for prioritizing and planning the change, and for engaging and communicating with the stakeholders12. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 4: Ensure that a continual improvement process is in place to maintain and enhance the performance and maturity of IT governance.

Question: 67

Which of the following is MOST critical for the successful implementation of an IT process?

A. Process framework
B. Service delivery process model
C. Objectives and metrics
D. IT process assessment

Answer: C

Explanation:

Objectives and metrics are the most critical for the successful implementation of an IT process, as they define the purpose, scope, and expected outcomes of the process. Objectives and metrics also help to measure and monitor the performance, efficiency, and effectiveness of the process,and to identify and implement improvement opportunities12. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic C: Technology Governance, Task 2: Ensure that IT processes are defined, implemented, monitored and continually improved in alignment with the enterprise governance framework.

Question: 68

The board of directors has mandated the use of geolocation software to track mobile assets assigned to employees who travel outside of their home country. To comply with this mandate, the IT steering committee should FIRST request

A. the inclusion of mandatory training for remote device users.
B. an architectural review to determine appropriate solution design.
C. an assessment to determine if data privacy protection is addressed.
D. an update to the acceptable use policy.

Answer: C

Explanation:

An assessment to determine if data privacy protection is addressed is the first request that the IT steering committee should make to comply with the board's mandate, as it helps to ensure that the use of geolocation software does not violate any applicable laws, regulations, or ethical standards regarding the collection, processing, and sharing of personal or sensitive data. Data privacy protection is an important aspect of information governance, which is part of the CGEIT Domain 1: Governance of Enterprise IT1. An assessment can also identify the risks and controls associated with the geolocation software, and provide recommendations and best practices for its implementation and management2. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic C: Information Governance, Task 1: Define and implement information governance processes to ensure alignment with enterprise goals and objectives.

Question: 69

An analysis of an organization s security breach is complete. The results indicate that the quality of the code used for updates to its primary customer-facing software has been declining and security flaws were introduced. The FIRST IT governance action to correct this problem should be to review: A. compliance with the user testing process.

B. the change management control framework.
C. the qualifications of developers to write secure code.
D. the incident response plan.

Answer: B

Explanation:

The change management control framework is the first IT governance action to correct the problem of declining code quality and security flaws, as it defines and implements the policies, procedures, and standards for managing changes to the IT systems and software. The change management control framework also ensures that changes are authorized, tested, documented, and deployed in a consistent and secure manner12. A review of the change management control framework can help to identify and address the root causes of the security breach, and to prevent or mitigate similar incidents in the future. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic C: Technology Governance, Task 3: Ensure that IT processes are compliant with relevant laws, regulations and contractual requirements.

Question: 70

Which of the following is the MOST effective way of assessing enterprise risk?

A. Business impact analysis (BIA)
B. Business vulnerability assessment
C. Likelihood of threat analysis
D. Operational risk assessment

Answer: D

Explanation:

An operational risk assessment is the most effective way of assessing enterprise risk, as it evaluates the potential losses and impacts that may arise from inadequate or failed internal processes, people, systems, or external events. An operational risk assessment also helps to identify and prioritize the key risk indicators (KRIs), risk scenarios, and mitigation strategies for the enterprise12. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 1: Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework.

Question: 71

A CIO must determine if IT staff have adequate skills to deliver on key strategic objectives. Which of the following will provide the MOST useful information?

A. Employee performance metrics
B. Project risk reports
C. Gap analysis results
D. Training program statistics

Answer: C

Explanation:

Gap analysis results will provide the most useful information for the CIO to determine if IT staff have adequate skills to deliver on key strategic objectives, as they compare the current state ofthe IT staff skills with the desired or required state. Gap analysis results also help to identify the gaps or deficiencies in the IT staff skills, and to plan and implement the actions and strategies to close or reduce the gaps1. A gap analysis can be performed using various methods and tools, such as SWOT analysis, skill matrix, competency framework, etc.

Question: 72

When evaluating benefits realization of IT process performance, the analysis MUST be based on;

A. key business objectives.
B. industry standard key performance indicators (KPIs).
C. portfolio prioritization criteria.
D. IT risk policies.

Answer: A

Explanation:

When evaluating benefits realization of IT process performance, the analysis must be based on key business objectives, as they define the desired outcomes and value that the IT processes are expected to deliver and support. Key business objectives are derived from the enterprise strategy and vision, and they provide the basis

for measuring and monitoring the IT process performance and benefits123. Reference := CGEIT Exam Content Outline, Domain 3, Subtopic B: Performance Measurement and Optimization, Task 1: Establish and monitor IT performance measurement systems to evaluate the extent to which IT delivers on its strategic objectives and desired outcomes.

Question: 73

Which of the following is the PRIMARY ongoing responsibility of the IT governance function related to risk?

A. Responding to and controlling all IT risk events
B. Communicating the enterprise risk management plan
C. Ensuring IT risk management is aligned with business risk appetite
D. Verifying that all business units have staff skilled at assessing risk

Answer: C

Explanation:

Ensuring IT risk management is aligned with business risk appetite is the primary ongoing responsibility of the IT governance function related to risk, as it helps to ensure that the IT risks are consistent with the enterprise's objectives, strategy, and tolerance for risk. IT risk management alignment also facilitates the integration of IT risk management with enterprise risk management (ERM), and the communication and reporting of IT risk to the relevant stakeholders123. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 1: Ensure that an IT risk management framework exists to identify, analyze,mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework.

Question: 74

An enterprise considering implementing IT governance should FIRST develop the scope of the IT governance program and:

A. initiate the program using an implementation roadmap.
B. establish initiatives for business and managers.
C. acquire the resources that will be required.
D. communicate the program to stakeholders to gain consensus.

Answer: D

Explanation:

Communicating the program to stakeholders to gain consensus is the first step after developing the scope of the IT governance program, as it helps to ensure that the program is aligned with the enterprise goals and objectives, and that it has the support and commitment of the key parties who have an interest or influence in the IT governance. Communication also helps to overcome resistance, address concerns, and foster collaboration among the stakeholders12. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 3: Ensure that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Question: 75

Which of the following should be the MAIN reason for an enterprise to implement an IT risk management framework?

A. The need to enable IT risk-aware decisions by executives
B. The results of an external audit report concerning IT risk management processes.

C. The need to address market regulations and internal compliance in IT risk
D. The ability to benchmark IT risk policies against major competitors

Answer: A

Explanation:

The main reason for an enterprise to implement an IT risk management framework is the need to enable IT risk-aware decisions by executives, as it helps to ensure that the IT risks are aligned with the enterprise strategy, objectives, and risk appetite. IT risk management also provides a consistent and structured approach to identify, analyze, treat, and monitor IT-related business risks, and to communicate and report them to the relevant stakeholders12. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 1: Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor, andcommunicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework.

Question: 76

An enterprise's information security function is making changes to its data retention and backup policies. Which of the following presents the GREATEST risk?

A. Business data owners were not consulted.
B. The new policies Increase the cost of data backups.
C. Data backups will be hosted at third-party locations.
D. The retention period for data backups is Increased.

Answer: A

Explanation:

Business data owners were not consulted is the answer that presents the greatest risk, as it implies that the information security function did not consider the needs, expectations, and requirements of the stakeholders who are responsible for the data. Business data owners should be involved in the development and implementation of data retention and backup policies, as they can provide input on the value, sensitivity, and classification of the data, as well as the legal and regulatory obligations for data preservation and protection12. Without consulting the business data owners, the information security function may create policies that are inconsistent, ineffective, or detrimental to the enterprise’s objectives and operations.

Question: 77

Which of the following would be MOST important to update if a decision is made to ban end user- owned devices in the workplace?

A. Employee nondisclosure agreement
B. Enterprise risk appetite statement
C. Enterprise acceptable use policy
D. Orientation training materials

Answer: C

Explanation:

An enterprise acceptable use policy is the most important document to update if a decision is made to ban end user-owned devices in the workplace, as it defines and communicates the rules and guidelines for the appropriate and secure use of IT resources and services by the employees and other authorized users. An enterprise acceptable use policy also helps to protect the enterprise’s data, assets, and reputation from

unauthorized or malicious access, disclosure, or damage12.

Updating the enterprise acceptable use policy to reflect the ban on end user-owned devices can help to ensure compliance, awareness, and enforcement of the decision. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic C: InformationGovernance, Task 2: Ensure that information governance processes are aligned with the enterprise risk management (ERM) processes.

Question: 78

Which of the following is the MOST effective way to manage risks within the enterprise?

A. Assign individuals responsibilities and accountabilities for management of risks.
B. Make staff aware of the risks in their area and risk management techniques.
C. Provide financial resources for risk management systems.
D. Document procedures and reporting processes.

Answer: A

Explanation:

Assigning individuals responsibilities and accountabilities for management of risks is the most effective way to manage risks within the enterprise, as it ensures that the risk owners and stakeholders are clearly identified, involved, and accountable for the risk management activities and outcomes. Assigning responsibilities and accountabilities also helps to establish roles and expectations, delegate authority, and monitor performance and compliance12. Reference := CGEIT Exam Content Outline, Domain 4, Subtopic B: IT Risk Management, Task 2: Ensure that appropriate senior level management sponsorship for IT risk management exists.

Question: 79

Which of the following is an ADVANTAGE of using strategy mapping?

A. It provides effective indicators of productivity and growth.
B. It depicts the maturity levels of processes that support organizational strategy.
C. It identifies barriers to strategic alignment and links them to specific outcomes.
D. It depicts the cause-and-effect linked relationships between strategic objectives.

Answer: D

Explanation:

Strategy mapping is an advantage of using strategy mapping, as it helps to visualize and communicate how the enterprise can create value by achieving its strategic objectives. Strategy mapping also helps to align the IT goals and activities with the enterprise strategy, and to measure and monitor the IT performance and outcomes123. Reference := CGEIT Exam Content Outline, Domain 3, Subtopic A: Performance Management, Task 2: Ensure that IT performance measurement supports IT performance management by providing relevant, complete, reliable, timely and consistent information.

Question: 80

Due to continually missed service level agreements (SLAs), an enterprise plans to terminate its contract with a vendor providing IT help desk services. The enterprise s IT department willassume the help desk-related responsibilities. Which of the following would BEST facilitate this transition? A. Requiring the enterprise architecture (EA) be updated

B. Validating that the balanced scorecard is still meaningful
C. Ensuring IT will operate at a lower cost than the vendor
D. Ensuring a change management plan is in place

Answer: D

Explanation:

Ensuring a change management plan is in place is the best way to facilitate the transition from a vendor providing IT help desk services to the enterprise's IT department, as it helps to define and implement the steps, activities, and resources needed to achieve the change objectives. A change management plan also helps to manage the risks, issues, and impacts of the change, and to communicate and coordinate with the stakeholders and staff involved in the change123. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic C: Technology Governance, Task 3: Ensure that IT processes are compliant with relevant laws, regulations and contractual requirements.

Question: 81

A manufacturing company has recently decided to outsource portions of its IT operations. Which of the following would BEST justify this decision?

A. Core legacy systems are not fully integrated with enterprise IT systems.
B. Business users are not able to decide upon IT service levels to be provided.
C. Increasing complexity of core business and IT processes have led to dramatic increasing costs.
D. The business strategy requires significant IT resource scalability over the next five years.

Answer: D

Explanation:

The business strategy requiring significant IT resource scalability over the next five years is the best justification for the decision to outsource portions of IT operations, as it implies that the manufacturing company needs to adapt to changing market demands, customer expectations, and business opportunities. Outsourcing IT operations can provide the company with access to external IT resources, such as infrastructure, software, and services, that can be scaled up or down according to the business needs and goals12. Outsourcing IT operations can also help the company to reduce costs, improve efficiency, and focus on its core competencies

Question: 82

A CIO believes that a recent mission-critical IT decision by the board of directors is not in the best financial interest of all stakeholders. Which of the following is the MOST ethical course of action? A. Share concerns with the legal department.

B. Request a meeting with the board.
C. Engage an independent cost-benefit analysis.
D. Request an internal audit review of the board's decision.

Answer: B

Explanation:

Requesting a meeting with the board is the most ethical course of action for the CIO who believes that a recent mission-critical IT decision by the board of directors is not in the best financial interest of all stakeholders, as it allows the CIO to express their concerns and opinions in a respectful and professional manner, and to provide relevant information and evidence to support their views. Requesting a meeting with the board also demonstrates the CIO's commitment and accountability to the enterprise's goals and values, and their willingness to collaborate and communicate with the board on IT governance matters123. Reference := CGEIT Exam Content Outline, Domain 1, Subtopic A: Governance Framework, Task 3: Ensure that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance

against agreed-on direction and objectives.

Question: 83

A retail enterprise has cost reduction as its top priority. From a governance perspective, which of the following should be the MOST important consideration when evaluating different IT investment options?

A. Support for increased sales
B. Risk associated with each option
C. Industry best practices
D. Business value impact

Answer: D

Explanation:

The most important consideration for IT governance is to align IT investments with business objectives and deliver value to the enterprise. Cost reduction is one of the possible objectives, but not the only one. Therefore, the business value impact of each option should be evaluated to ensure that the IT investment supports the enterprise strategy and goals. Reference:= CGEIT Exam Content Outline, Domain 1: Governance of Enterprise IT, Subtopic A: Governance Framework, Task 1: Establish and maintain a governance framework that aligns with enterprise objectives, ensures value creation from IT-enabled investments, and manages risk at an acceptable level.

Question: 84

Which of the following is the MOST important consideration for data classification to be successfully implemented?

A. Users should be provided with clear instructions that are easy to follow and understand.
B. The data classification tools integrate with other tools that help manage the data.
C. The classification scheme should be closely aligned with the IT strategic plan.
D. Senior management should be properly trained in monitoring compliance.

Answer: A

Explanation:

Data classification is a process that involves users assigning labels or tags to data based on its sensitivity, value, and protection requirements. Users are the ones who know the data best and are responsible for handling it appropriately. Therefore, users should be provided with clear instructions that are easy to follow and understand, so they can classify data correctly and consistently. This will also help users comply with the data security policies and regulations that apply to the data they work with. Reference := CGEIT Exam Content Outline, Domain 1: Governance of Enterprise IT, Subtopic B: IT Resources, Task 3: Ensure that processes are in place to maintain the integrity, availability, reliability, performance, scalability and security of IT resources. What is Data Classification? | Best Practices & Data Types | Imperva, User-based classification section. Best practices for data classification - ManageEngine, 6 best practices for data classification section.

Question: 85

Which of the following BEST reflects the ethical values adopted by an IT organization?

A. IT principles and policies
B. IT balanced scorecard
C. IT governance framework
D. IT goals and objectives

Answer: A

Explanation:

IT principles and policies are the documents that best reflect the ethical values adopted by an IT organization. IT principles are the high-level statements that express the fundamental beliefs and values of the organization regarding the use and management of IT. IT policies are the specific rules and guidelines that implement the IT principles and ensure compliance with ethical standards and regulations. IT principles and policies help to align IT with business objectives, foster a culture of trust and responsibility, and promote good governance practices.
Reference := CGEIT Exam Content Outline, Domain 1: Governance of Enterprise IT, Subtopic A: Governance Framework, Task 2: Ensure that a framework is in place to support the alignment of IT with enterprise objectives, enabling value creation. Ethics for IT Professionals/ProfessionalCode of Ethics, Ethical Code section. Values and Ethics in Information Systems, Introduction section. Purpose, Ethical Values, Culture and Behaviours, Ethical Values section.

Question: 86

Which of the following would provide the BEST input for prioritizing strategic IT improvement initiatives?

A. Business dependency assessment
B. Business process analysis
C. Business case evaluation
D. Business impact analysis (BIA)

Answer: C

Explanation:

A business case evaluation is the best input for prioritizing strategic IT improvement initiatives because it provides a clear and objective assessment of the costs, benefits, risks, and value of each initiative. A business case evaluation helps to compare different options and select the ones that align with the organization's goals, strategy, and budget. A business case evaluation also helps to
justify the investment and secure the support and approval from the stakeholders.
A business dependency assessment is a process that identifies the critical business functions and processes that rely on IT services and resources. It helps to determine the impact of IT disruptions or failures on the business continuity and recovery. A business dependency assessment is useful for IT risk management and disaster recovery planning, but not for prioritizing strategic IT improvement initiatives.
A business process analysis is a method that examines the current state of the business processes, identifies the gaps, inefficiencies, and opportunities for improvement, and proposes solutions to optimize the processes. A business process analysis helps to streamline the workflows, reduce costs, increase quality, and enhance customer satisfaction. A business process analysis is valuable for IT process improvement and automation, but not for prioritizing strategic IT improvement initiatives. A business impact analysis (BIA) is a technique that evaluates the potential consequences of a disruption or disaster on the organization's operations, assets, reputation, and stakeholders. It helps to estimate the financial and nonfinancial losses, recovery time objectives, recovery point objectives, and criticality levels of each business function and process. A BIA is essential for IT business continuity management and contingency planning, but not for prioritizing strategic IT improvement initiatives.
Reference := IT Strategy Examples & Best Practices — IT Companies Network, How to create an IT strategy plan section. What is an IT Roadmap? | Benefits and Roadmap Examples - ProductPlan, How to Prioritize Your IT Roadmap section. 7 ways to make IT operations more efficient | CIO, Use data to increase visibility section.

Question: 87

What is the PRIMARY objective for performing an IT due diligence review prior to the acquisition of a competitor?

A. Document the competitor's governance structure.
B. Ensure that the competitor understands significant IT risks.
C. Assess the status of the risk profile of the competitor.
D. Determine whether the competitor is using industry-accepted practices.

Answer: C

Explanation:

The primary objective for performing an IT due diligence review prior to the acquisition of a competitor is to assess the status of the risk profile of the competitor. IT due diligence is a process that evaluates the technology assets, capabilities, processes, and security of a target company. It helps to identify any potential risks, liabilities, gaps, or issues that could affect the value, integration, or performance of the acquisition. IT due diligence also helps to determine the synergies, opportunities, and costs of combining or separating the IT systems and resources of both companies. By conducting an IT due diligence review, the acquirer can gain a comprehensive understanding of the competitor's IT environment and make informed decisions about the deal.

Documenting the competitor's governance structure, ensuring that the competitor understands significant IT risks, and determining whether the competitor is using industry-accepted practices are not the primary objectives for performing an IT due diligence review. These are possible outcomes or benefits of the review, but they are not the main purpose or goal. The primary objective is to assess the risk profile of the competitor and its impact on the acquisition.

Reference := IT Due Diligence Checklist: Must-Assess Technology Elements Prior to Any Acquisition - Performance Improvement Partners Blog, Introduction section. IT Due Diligence: How to Do It Right (+ Checklist) - DealRoom, What is IT due diligence? section. IT Due Diligence | Optimising IT, Introduction section. Reviewing It In Due Diligence, Overview section.

Question: 88

The IT program manager does not see the value of conducting risk assessments for a new major IT project. The manager is reluctant to cooperate with internal auditors and the newly formed steering committee. Midway through the project, program requirements were changed because the CEO is a friend of a vendor and wants to implement this vendor's new technology. This decision will cause the current IT program budget to be insufficient and will be shown as overspending.

After the requirement change request, the IT program manager should FIRST:

A. obtain confirmation from the business and a decision by the steering committee.
B. request additional funding from the business owner to cover the additional scope.
C. report the matter to internal audit as a program deviation to be reviewed.
D. align IT with the business and agree to the business request.

Answer: A

Explanation:

The IT program manager should first obtain confirmation from the business and a decision by the steering committee before proceeding with the requirement change request. This is because the requirement change request is a major scope change that will affect the program budget, schedule, quality, and risk. The IT program manager needs to ensure that the business owner and the steering committee are aware of the implications

and benefits of the change, and that they approve it formally. The IT program manager also needs to follow the established change management process and document the change request and its approval.
Requesting additional funding from the business owner to cover the additional scope is not the first step, as it assumes that the change request is already approved and justified. The IT program manager should first seek confirmation and approval from the business owner and the steering committee before asking for more resources.
Reporting the matter to internal audit as a program deviation to be reviewed is not the first step, as it implies that the change request is a violation or a problem. The IT program manager should first communicate with the business owner and the steering committee to understand their rationale and expectations for the change request, and to present the impact analysis and alternatives.
Aligning IT with the business and agreeing to the business request is not the first step, as it disregards the role and authority of the steering committee. The IT program manager should not accept or reject the change request without consulting with the steering committee, which is responsible for overseeing and governing the program.
Reference := Program Management Best Practices | Smartsheet, Best Practices for Running an Ongoing Program section. Program Management: 8 Tips & Tricks for Success (Update 2023), Tip 2: Defining the control processes section. Program Management Best Practices - Project Management Institute, Comprehend the differences between programs and projects section.

Question: 89

An enterprise is planning a change in business direction. As a result, IT risk will significantly increase.
Which of the following should be the GO'S FIRST course of action?

A. Recommend delaying the business change.
B. Implement IT changes to align with the plan.
C. Report the risk to executive management
D. Plan for the corresponding IT reorganization.

Answer: C

Explanation:

The CIO's first course of action should be to report the risk to executive management, as they are ultimately responsible for the strategic direction and risk appetite of the enterprise. Reporting the risk will help to ensure that executive management is aware of the potential impact and consequences of the change in business direction, and that they can make informed decisions about how to proceed. Reporting the risk will also help to establish a clear communication channel and a collaborative relationship between the IT function and the business function, which are essential for effective IT governance and risk management.
Recommending delaying the business change is not the first course of action, as it may not be feasible or desirable for the enterprise. The CIO should not interfere with the business objectives or priorities without first understanding the rationale and expectations of executive management. The CIO should also not assume that the risk is unacceptable or unmanageable without conducting a proper risk assessment and analysis.
Implementing IT changes to align with the plan is not the first course of action, as it may be premature or inappropriate for the IT function to act on the change in business direction without first consulting with executive management and other stakeholders. The CIO should not initiate or approve any IT changes without first understanding the scope, requirements, benefits, and risks of the change, and without following the established change management process and procedures. Planning for the corresponding IT reorganization is not the first course of action, as it may be unnecessary or counterproductive for the IT function to restructure its resources, roles, and responsibilities without first communicating with executive management and other stakeholders. The CIO should not assume that the change in business

direction will require a major IT reorganization without first evaluating the current and future state of the IT environment, and without considering the impact on the IT performance, efficiency, and effectiveness.
Reference := IT Risk Resources | ISACA, Risk Management Best Practices section. IT Risk Management Process & Frameworks - ProjectManager, How to Manage Risk in IT section. Complete Guide to IT Risk Management | CompTIA, How to Implement an Effective Risk Management Strategy section. IT Risk Management Best Practices | Risk Management Strategies, Continuous Evaluation section. 6 Best Practices in Cybersecurity Risk Management - Indusface, Communication of Risks section.

Question: 90

Which of the following is MOST important to effectively initiate IT-enabled change?

A. Establish a change management process.
B. Obtain top management support and ownership.
C. Ensure compliance with corporate policy.
D. Benchmark against best practices.

Answer: B

Explanation:

The most important factor to effectively initiate IT-enabled change is to obtain top management support and ownership. This is because top management can provide the vision, direction, resources, and authority for the change, as well as communicate the benefits and urgency of the change to the rest of the organization. Top management support and ownership can also help to overcome resistance, align stakeholders, and ensure accountability and governance for the change. According to a McKinsey survey1, having active and visible executive sponsorship is the most important practice for successful digital transformations.
Establishing a change management process is also important, but not the most important factor. A change management process can help to plan, execute, monitor, and control the change activities, as well as address the human side of the change. However, without top management support and ownership, a change management process may not be effective or sustainable.
Ensuring compliance with corporate policy is also important, but not the most important factor. Compliance with corporate policy can help to ensure that the change is consistent with the organization's values, standards, and regulations, as well as avoid legal or ethical issues. However, compliance with corporate policy may not be sufficient or relevant for initiating IT-enabled change, especially if the policy is outdated or incompatible with the change objectives.
Benchmarking against best practices is also important, but not the most important factor. Benchmarking against best practices can help to identify gaps, opportunities, and solutions for improving the organization's performance and competitiveness through IT-enabled change. However, benchmarking against best practices may not be applicable or feasible for initiating IT- enabled change, especially if the change is innovative or disruptive.
Reference := The Magic Bullet Theory in IT-Enabled Transformation, Introduction section. The keys to a successful digital transformation | McKinsey, The anatomy of digital transformations section. Best Practices in Change Management - Prosci, Introduction section.

Question: 91

Which of the following would BEST help to improve an enterprise's ability to manage large IT investment projects?

A. Creating a change management board
B. Reviewing and evaluating existing business cases

C. Implementing a review and approval process for each phase
D. Publishing the IT approval process online for wider scrutiny

Answer: C

Explanation:

Implementing a review and approval process for each phase would best help to improve an enterprise's ability to manage large IT investment projects. This is because a review and approval process can help to ensure that the project is aligned with the business objectives, scope, budget, schedule, quality, and risk criteria at each stage of the project life cycle. A review and approval process can also help to monitor the project progress, performance, and deliverables, as well as identify and resolve any issues or changes that may arise. A review and approval process can also provide transparency, accountability, and governance for the project stakeholders and decisionmakers.

Creating a change management board is not the best answer, as it is only one aspect of a review and approval process. A change management board is a group of people who are responsible for reviewing, approving, or rejecting change requests that affect the project scope, schedule, cost, or quality. A change management board is important for managing changes in a project, but it is not sufficient or comprehensive for managing large IT investment projects.

Reviewing and evaluating existing business cases is not the best answer, as it is only a preliminary step in a review and approval process. A business case is a document that provides the justification and rationale for initiating a project, based on the expected costs, benefits, risks, and value of the project. Reviewing and evaluating existing business cases can help to select and prioritize the most viable and valuable projects for the enterprise, but it is not enough or relevant for managing large IT investment projects.

Publishing the IT approval process online for wider scrutiny is not the best answer, as it is only a communication method for a review and approval process. Publishing the IT approval process online can help to increase the visibility, awareness, and understanding of the project requirements, criteria, and procedures among the project stakeholders and participants. Publishing the IT approval process online can also help to solicit feedback, suggestions, or concerns from the wider audience. However, publishing the IT approval process online does not necessarily improve the enterprise's ability to manage large IT investment projects.

Reference := IT Portfolio Management Strategies | Smartsheet, Managing an IT portfolio requires four steps section. Best Practices in Project Management | Smartsheet, Establish ground rules for how the project will move forward section. Government of Canada project management - Canada.ca, These practices include establishing clear accountabilities section. IT Project Management: Concepts, Solutions & Best Practices, What is Integrated Project Management (IPM)? section. 16 Industry Experts Share Best Practices For IT Project Management - Forbes, 1. Limit Work In Progress section.

Question: 92

A business case indicates an enterprise would reduce costs by implementing a bring your own device (BYOD) program allowing employees to use personal devices for email. Which of the following should be the FIRST governance action?

A. Assess the enterprise architecture (EA).
B. Update the network infrastructure.
C. Update the BYOD policy.
D. Assess the BYOD risk.

Answer: D

Explanation:

The first governance action for implementing a BYOD program should be to assess the BYOD risk. This is because BYOD introduces various security, legal, and operational risks to the enterprise, such as data loss or leakage, unauthorized access, malware infection, compliance violation, device management, and user privacy. Assessing the BYOD risk can help to identify and evaluate the potential threats, vulnerabilities, and impacts of allowing employees to use personal devices for email. Assessing the BYOD risk can also help to determine the appropriate controls and mitigation strategies to reduce the risk to an acceptable level.

Assessing the enterprise architecture (EA) is not the first governance action, as it is a subsequent step after assessing the BYOD risk. EA is a framework that defines the structure, components, relationships, and principles of the enterprise's IT environment. Assessing the EA can help to ensure that the BYOD program aligns with the enterprise's vision, strategy, goals, and standards. However, assessing the EA does not address the specific risks associated with BYOD.

Updating the network infrastructure is not the first governance action, as it is an implementation step after assessing the BYOD risk and EA. Updating the network infrastructure can help to enhance the performance, reliability, scalability, and security of the network that supports the BYOD program. However, updating the network infrastructure does not provide a comprehensive risk assessment or

governance framework for BYOD.

Updating the BYOD policy is not the first governance action, as it is a result of assessing the BYOD risk and EA. A BYOD policy is a document that defines the rules, guidelines, and responsibilities for employees who use personal devices for email. Updating the BYOD policy can help to communicate the expectations and requirements for BYOD users and enforce compliance and accountability. However, updating the BYOD policy does not provide a thorough risk analysis or architectural alignment for BYOD.

Reference := BYOD Best Practices - JumpCloud, Assessing your needs section. End user device security for Bring-Your-Own-Device (BYOD) deployment models - ITSM.70.003 - Canadian Centre for Cyber Security, 1 Introduction section. BYOD Policy Best Practices: The Ultimate Checklist - Scalefusion, Introduction section. The Ultimate Guide to BYOD Security: Definition & More - Digital Guardian, The Challenges of BYOD Security section.

Question: 93

The CIO of a financial services company is tasked with ensuring IT processes are in compliance with recently instituted regulatory changes. The FIRST course of action should be to:

A. align IT project portfolio with regulatory requirements.
B. create an IT balanced scorecard.
C. identify the penalties for noncompliance.
D. perform a current state assessment.

Answer: D

Explanation:

The first course of action for the CIO of a financial services company to ensure IT processes are in compliance with recently instituted regulatory changes should be to perform a current state assessment. This is because a current state assessment can help to evaluate the existing IT processes, policies, controls, and performance against the new regulatory requirements and identify any gaps, issues, or risks that need to be addressed. A current state assessment can also help to establish a baseline and a benchmark for measuring the progress and effectiveness of the compliance initiatives.

Aligning IT project portfolio with regulatory requirements is not the first course of action, as it is a subsequent step after performing a current state assessment. Aligning IT project portfolio with regulatory requirements can help to prioritize and allocate resources for the IT projects that support the compliance objectives and deliver value to the business. However, aligning IT project portfolio with regulatory requirements requires a clear

understanding of the current state and the desired state of the IT processes and compliance.

Creating an IT balanced scorecard is not the first course of action, as it is a tool for monitoring and reporting the compliance outcomes and impacts. An IT balanced scorecard is a framework that measures and communicates the performance of the IT function in terms of financial, customer, internal process, and learning and growth perspectives. An IT balanced scorecard can help to align the IT strategy with the business strategy, track the progress and results of the IT initiatives, and demonstrate the value and contribution of IT to the business. However, creating an IT balanced scorecard does not provide a comprehensive analysis or improvement plan for the IT processes and compliance.

Identifying the penalties for noncompliance is not the first course of action, as it is only a motivation factor for compliance. Identifying the penalties for noncompliance can help to raise awareness and urgency of the compliance issues and risks, as well as deter or prevent violations or breaches.

However, identifying the penalties for noncompliance does not provide a detailed assessment or guidance for achieving compliance.

Reference := IT Compliance: What You Need to Know | Smartsheet, How to Achieve Compliance section. IT Compliance Management Best Practices: 5 Tips from Experts - MetricStream, Tip 1: Assess your current state section. IT Compliance Checklist: How to Ensure Your Business Is Compliant - Blissfully, Step 1: Assess Your Current State section. IT Compliance Management - Definition & Overview | OpsCompass, How Do You Manage IT Compliance? section.

Question: 94

The CIO of an enterprise learns the payroll server of a competitor has been the victim of ransomware. To help plan for the possibility of ransomed corporate data, what should be the CIO's FIRST course of action?

A. Require development of key risk indicators (KRIs).
B. Develop a policy to address ransomware.
C. Request a targeted risk assessment.
D. Back up corporate data to a secure location.

Answer: C

Explanation:

The first course of action for the CIO of an enterprise to help plan for the possibility of ransomed corporate data should be to request a targeted risk assessment. This is because a targeted risk assessment can help to identify and evaluate the specific threats, vulnerabilities, and impacts of ransomware attacks on the enterprise's data and systems. A targeted risk assessment can also help to determine the likelihood and severity of ransomware incidents, as well as the appropriate controls and mitigation strategies to reduce the risk to an acceptable level.

Requiring development of key risk indicators (KRIs) is not the first course of action, as it is a monitoring tool for measuring the risk exposure and performance. KRIs are metrics that provide information on the current level and trend of risk in relation to the risk appetite and tolerance of the enterprise. KRIs can help to track and report the progress and effectiveness of the risk management activities, as well as alert the management of any potential issues or changes that may affect the risk profile. However, requiring development of KRIs does not provide a comprehensive analysis or improvement plan for ransomed corporate data.

Developing a policy to address ransomware is not the first course of action, as it is a result of conducting a targeted risk assessment. A policy to address ransomware is a document that defines the rules, guidelines, and responsibilities for preventing, detecting, responding to, and recovering from ransomware attacks. Developing a policy to address ransomware can help to communicate the expectations and

requirements for ransomware protection and compliance, as well as enforce accountability and governance for ransomware incidents. However, developing a policy to address ransomware does not provide a detailed assessment or guidance for ransomed corporate data. Backing up corporate data to a secure location is not the first course of action, as it is an implementation step after conducting a targeted risk assessment and developing a policy to address ransomware. Backing up corporate data to a secure location can help to preserve the availability, integrity, and confidentiality of the data in case of a ransomware attack. Backing up corporate data to a secure location can also help to restore the data and resume normal operations after a ransomware attack. However, backing up corporate data to a secure location does not provide a thorough risk analysis or governance framework for ransomed corporate data.

Reference := Ransomware Risk Management: NISTIR 8374, 3 Risk Management Process section. Managing the Risks of Ransomware - SEI Blog, Assess Your Risk section. Ransomware Risk Management - NIST, 4 Ransomware Risk Management Profile section. NIST Releases Tips and Tactics for Dealing With Ransomware, Back Up Your Data section.

Question: 95

Which of the following aspects of the transition from X-rays to digital images would be BEST addressed by implementing information security policy and procedures?

A. Establishing data retention procedures
B. Training technicians on acceptable use policy
C. Minimizing the impact of hospital operation disruptions on patient care
D. Protecting personal health information

Answer: D

Explanation:

The aspect of the transition from X-rays to digital images that would be best addressed by implementing information security policy and procedures is protecting personal health information. This is because personal health information is a type of sensitive data that contains confidential and private information about patients, such as their medical history, diagnosis, treatment, and identity. Personal health information is subject to various legal and ethical obligations and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US1, that require its protection from unauthorized access, disclosure, modification, or destruction. Information security policy and procedures can help to define the rules, guidelines, and responsibilities for ensuring the confidentiality, integrity, and availability of personal health information in digital form. Establishing data retention procedures is not the best answer, as it is only one component of information security policy and procedures. Data retention procedures specify how long and where digital images should be stored, archived, or deleted, based on the business, legal, and regulatory requirements. Data retention procedures can help to optimize the storage capacity, performance, and cost of digital images, as well as comply with the applicable laws and regulations. However, data retention procedures do not address the full scope of information security policy and procedures. Training technicians on acceptable use policy is not the best answer, as it is only one aspect of information security policy and procedures. Acceptable use policy defines what are the permitted and prohibited behaviors and actions for using digital images and related IT resources. Training technicians on acceptable use policy can help to educate them on the security risks and best practices for handling digital images, as well as enforce compliance and accountability. However, training technicians on acceptable use policy does not cover the entire range of information security policy and procedures.

Minimizing the impact of hospital operation disruptions on patient care is not the best answer, as it is a business continuity objective rather than an information security objective. Business continuity refers to the ability of an organization to maintain or resume its critical functions and processes in the event of a disruption or disaster. Minimizing the impact of hospital operation disruptions on patient care can help to ensure the

safety, quality, and efficiency of health services delivery. However, minimizing the impact of hospital operation disruptions on patient care is not directly related to information security policy and procedures.
Reference := HIPAA Privacy Rule | HHS.gov, Introduction section. Information Security Policy: Definition & Examples - NetApp, What Is an Information Security Policy? section. Data Retention Policy: Definition & Best Practices - NetApp, What Is a Data Retention Policy? section. Acceptable Use Policy: Definition & Best Practices - NetApp, What Is an Acceptable Use Policy? section. [Business

Continuity Management: Definition & Best Practices - NetApp], What Is Business Continuity Management? section.

Question: 96

Prior to decommissioning an IT system, it is MOST important to:

A. assess compliance with environmental regulations.
B. assess compliance with the retention policy.
C. review the media disposal records.
D. review the data sanitation records.

Answer: B

Explanation:

This is because before decommissioning an IT system, it is most important to ensure that the data stored on the system is handled according to the retention policy of the organization. A retention policy is a document that specifies how long and where different types of data should be kept, archived, or deleted, based on the business, legal, and regulatory requirements. Assessing compliance with the retention policy can help to avoid data loss, leakage, or breach, as well as comply with the applicable laws and regulations.
Assessing compliance with environmental regulations is not the most important action, as it is a secondary consideration for decommissioning an IT system. Environmental regulations are rules that govern the disposal or recycling of IT equipment and materials, such as batteries, cables, or monitors, in order to protect the environment and human health. Assessing compliance with environmental regulations can help to reduce the environmental impact and waste of IT resources, as well as avoid fines or penalties. However, assessing compliance with environmental regulations does not address the primary concern of data management and security.
Reviewing the media disposal records is not the most important action, as it is a subsequent step after assessing compliance with the retention policy. Media disposal records are documents thatprovide evidence and verification of the proper disposal or destruction of IT media, such as hard drives, tapes, or disks, that contain sensitive or confidential data. Reviewing the media disposal records can help to ensure that the data on the IT system is erased or overwritten in a secure and irreversible manner, as well as comply with the audit and accountability requirements. However, reviewing the media disposal records does not provide a comprehensive assessment or guidance for data retention and compliance.
Reviewing the data sanitation records is not the most important action, as it is a similar step to reviewing the media disposal records. Data sanitation records are documents that provide evidence and verification of the proper sanitation or cleansing of data on an IT system, such as deleting, encrypting, or masking data that is no longer needed or relevant. Reviewing the data sanitation records can help to ensure that the data on the IT system is protected from unauthorized access, disclosure, modification, or destruction, as well as comply with the privacy and confidentiality requirements. However, reviewing the data sanitation records does not provide a thorough assessment or guidance for data retention and compliance.
Reference := Best Practices in Designing a Data Decommissioning Policy, Introduction section. Server Decommissioning: a Brief Guide and Checklist, Notify all relevant parties about server decommissioning section. Deconstructing Decommissioning: Best Practices for Managing the Final Mile of Critical Assets, Here

are seven best practices that when implemented can go a long way to ensure a successful decommissioning section. How to decommission a system: 3 keys to success - Enable Sysadmin, How to decommission a system: 3 keys to success section.

Question: 97

A CEO determines the enterprise is lagging behind its competitors in consumer mobile offerings, and mandates an aggressive rollout of several new mobile services within the next 12 months. To ensure the IT organization is capable of supporting this business objective, what should the CIO do FIRST?

A. Request an assessment of current in-house mobile technology skills.
B. Create a sense of urgency with the IT team that mobile knowledge is mandatory.
C. Procure contractors with experience in mobile application development.
D. Task direct reports with creating training plans for their teams.

Answer: A

Explanation:

The first thing the CIO should do to ensure the IT organization is capable of supporting the CEO's mandate of rolling out several new mobile services within the next 12 months is to request an assessment of current in-house mobile technology skills. This is because an assessment of current inhouse mobile technology skills can help to evaluate the existing level of knowledge, experience, and competence of the IT staff in developing, deploying, and maintaining mobile applications and services. An assessment of current in-house mobiletechnology skills can also help to identify any gaps, needs, or opportunities for improvement or enhancement of the IT staff's mobile technology skills.

Creating a sense of urgency with the IT team that mobile knowledge is mandatory is not the first thing the CIO should do, as it is a motivational factor rather than a governance factor. Creating a sense of urgency with the IT team can help to communicate the importance and priority of the CEO's mandate, as well as inspire and encourage the IT staff to learn and adopt mobile technology skills. However, creating a sense of urgency with the IT team does not provide a comprehensive analysis or improvement plan for the IT organization's mobile technology capabilities.

Procuring contractors with experience in mobile application development is not the first thing the CIO should do, as it is an implementation factor rather than a governance factor. Procuring contractors with experience in mobile application development can help to supplement or complement the in-house IT staff's mobile technology skills, as well as accelerate or facilitate the delivery and quality of the new mobile services. However, procuring contractors with experience in mobile application development does not address the long-term sustainability or scalability of the IT organization's mobile technology capabilities.

Tasking direct reports with creating training plans for their teams is not the first thing the CIO should do, as it is a subsequent step after requesting an assessment of current in-house mobile technology skills. Tasking direct reports with creating training plans for their teams can help to design and implement effective and customized learning programs and activities for the IT staff to acquire or enhance their mobile technology skills. However, tasking direct reports with creating training plans for their teams requires a clear understanding of the current state and the desired state of the IT staff's mobile technology skills.

Reference := Top 15 In-Demand Technology Skills (Plus Definition), Mobile Development section. How to Develop Mobile Technology Skills | Career Trend, Step 1 section. How To Build A Mobile App Development Team - Forbes, Introduction section.

Question: 98

Which of the following is the MOST effective way for a CIO to govern business unit deployment of shadow IT applications in a cloud environment?

A. Implement controls to block the installation of unapproved applications.
B. Educate the executive team about the risk associated with shadow IT applications.

C. Provide training to the help desk to identify shadow IT applications.
D. Review and update the application implementation process.

Answer: B

Explanation:

The most effective way for a CIO to govern business unit deployment of shadow IT applications in a cloud environment is to educate the executive team about the risk associated with shadow ITapplications. This is because shadow IT applications are often deployed without the knowledge or approval of the central IT organization, and may pose security, compliance, and performance risks to the enterprise. By raising awareness of these risks among the executive team, the CIO can foster a culture of IT governance and alignment, and encourage the business units to follow the established application implementation process. Reference: CGEIT Certification | Certified in Governance of Enterprise IT | ISACA1, IT Governance: Definitions, Frameworks and Planning - ProjectManager2

Question: 99

Before an IT strategy committee can approve an IT risk assessment framework, which of the following is MOST important to have established?

A. An enterprise risk mitigation strategy
B. Leading and lagging risk indicators
C. IT performance metrics and standards
D. Enterprise definitions for risk impact and probability

Answer: D

Explanation:

Before an IT strategy committee can approve an IT risk assessment framework, the most important thing to have established is enterprise definitions for risk impact and probability. This is because a risk assessment framework is an approach for prioritizing and sharing information about the security risks posed to an information technology organization1. To do this effectively, the organization needs to have a common understanding of how to measure and communicate the likelihood and consequences of different risks. Without consistent definitions for risk impact and probability, the risk assessment framework might not be aligned with the enterprise's risk appetite and tolerance, and might not provide meaningful or actionable results. Reference: Risk Assessment Framework (RAF) - CIO Wiki1, IT Risk Resources | ISACA2, 5 IT risk assessment frameworks compared | CSO Online

Question: 100

An IT governance committee wants to ensure there is a clear description of the "data owner" in the enterprise data policy. Which of the following would BEST define the owner of data stored in an external cloud?

A. The business leader who is most impacted by the loss of data.
B. The risk manager who is responsible for protecting data stored in the cloud.
C. The contract manager who monitors the security of the cloud provider.
D. The vendor who submits the data to the organization via online forms

Answer: A

Explanation:

The owner of data stored in an external cloud is the business leader who is most impacted by the loss of data.

This is because the data owner is the person who has the accountability and authority over a specific dataset, and who is responsible for its security, quality, classification, and access control12. The data owner is usually a senior-level employee or a subject-matter expert who has the knowledge and motivation to ensure that the data is handled correctly and in compliance with policies and regulations2. The data owner is not the same as the data custodian, who is the person who implements the technical and operational measures to protect and manage the data according to the data owner's directives2. Therefore, the risk manager, the contract manager, and the vendor are not the data owners, as they do not have the final say or accountability over the data stored in the external cloud. Reference: What Is a Data Owner? - Firewall Times1, Data Owners vs. Data Stewards vs. Data Custodians - CPO Magazine2

Question: 101

A multinational enterprise recently purchased a large company located in a different country. When introducing the concept of governance to the new acquisition, it is MOST important that executive management recognize:

A. language differences.
B. the use of international standards.
C. the impact of cultural changes.
D. globally recognized good practices.

Answer: C

Explanation:

When introducing the concept of governance to the new acquisition, it is most important that executive management recognize the impact of cultural changes. This is because culture can influence how people understand and practice governance, and how they respond to different governance frameworks and policies1. Culture can also change over time, either by choice or by external factors, and this can affect the governance arrangements of an organization2. Therefore, executive management needs to be aware of the cultural differences and similarities between the multinational enterprise and the new acquisition, and how they can affect the governance objectives, processes, and outcomes. Executive management also needs to respect and value the cultural diversity of the new acquisition, and foster a culture of trust, collaboration, and alignment3. Reference: How corporate culture affects governance - The CEO Magazine3, Governance | Diversity of Cultural Expressions - UNESCO4, 2.0 Culture and governance - AIGI

Question: 102

The results of an internal audit show that the business and IT acquire resources differently, which causes duplicate purchases. Which of the following is the BEST way to address this issue?

A. Align IT objectives to the business procurement process.
B. Involve business in IT procurement decisions.
C. Establish a centralized procurement approval process.
D. Define roles and responsibilities through a RAG chart

Answer: C

Explanation:

The best way to address the issue of duplicate purchases caused by different acquisition methods of business and IT is to establish a centralized procurement approval process. A centralized procurement approval process is a process that organizations use to obtain approval for purchases that they intend to make. The process typically involves several steps, such as identifying a need, requesting a quote, obtaining quotes, and obtaining approval from a designated authority. By centralizing the procurement approval process, the organization can

avoid duplication, inconsistency, and inefficiency in purchasing decisions. A centralized procurement approval process can also help the organization to achieve the following benefits :

Visibility and control: The organization can have a clear view of all purchase requests and transactions, and can monitor and manage the budgets, requesters, and suppliers.

Better purchasing power: The organization can leverage its volume and history to negotiate better prices and discounts with vendors, and can establish long-term relationships with preferred suppliers.

Standardization: The organization can implement and enforce policies and standards for data quality, security, privacy, and usage, and can create a single source of truth for purchasing information. Eliminates maverick spending: The organization can identify and prevent individual spending that goes against the purchasing policies or that results in duplicate or unnecessary purchases.

Therefore, establishing a centralized procurement approval process is the best way to address the issue of duplicate purchases caused by different acquisition methods of business and IT. Reference: Centralized vs. Decentralized Purchasing: Key Differences | Pipefy, Centralizing Procurement: What Companies Need to Consider, What is the Procurement Approval Process: Detailed Guide

Question: 103

Which of the following is the MOST important benefit of developing an information architecture model consistent with enterprise strategy?

A. It identifies information architecture priorities.
B. It support and facilitates decision making.
C. It enables information architecture roadmap updates.
D. It optimizes information delivery and storage costs.

Answer: B

Explanation:

The most important benefit of developing an information architecture model consistent with enterprise strategy is that it supports and facilitates decision making. Information architecture is the part of the enterprise architecture process that describes the current state, future state, and guidance necessary to flexibly share and exchange information assets to achieve effective enterprise change1. Information architecture is an aspect of enterprise architecture that enables an information strategy or business solution through the definition of the company's business information assets, their sources, structure, classification and associations2. By developing an information architecture model that aligns with the enterprise strategy, the organization can ensure that the information assets are relevant, accurate, timely, and accessible for the decision makers. An information architecture model can also help the organization to identify information gaps, redundancies, and opportunities, and to prioritize information initiatives and investments. Moreover, an information architecture model can enable the organization to leverage its data and analytics capabilities to generate insights and value from the information assets. Therefore, developing an information architecture model consistent with enterprise strategy is crucial for supporting and facilitating decision making at all levels of the organization. Reference: Enterprise Business Strategy and Architecture | Deloitte US3, Business strategy modelling based on enterprise architecture: a state of the art review | Emerald Insight4, Enterprise Information Architecture (EIA) - CIO Wiki1, Data Architecture and Information Architecture: What's … - DATAVERSITY2

Question: 104

Which of the following is the BEST course of action to enable effective resource management?

A. Conduct an enterprise risk assessment.
B. Implement a cross-training program.
C. Assign resources based on business priorities.
D. Assign resources based on risk appetite.

Answer: C

Explanation:

The best course of action to enable effective resource management is to assign resources based on business priorities. Resource management is the process of enhancing efficiency and guiding the use of such project-critical resources as employees, equipment, and tools1. To manage resources effectively, it is important to align them with the business objectives and goals, and to allocate them according to the urgency and importance of the tasks2. By assigning resources based on business priorities, the organization can ensure that the most critical and valuable projects are completed on time and within budget, and that the resources are used optimally and productively3. Reference: 10 Best Practices for Effective Resource Management - Float2, What Is Resource
Management? Definition, Jobs, and More1, 10 Key Principles of Effective Resource Management - eResource Scheduler3

Question: 105

IT has launched new portfolio management policies and processes to improve the alignment of IT projects with enterprise goals. The latest audit report indicates that no improvement has been made due to confusion in the decision-making process. Which of the following is the BEST course of action for the CIO?

A. Deliver prioritization and facilitation training.
B. Implement a performance management framework.
C. Create an IT portfolio management risk framework.
D. Develop and communicate an accountability matrix.

Answer: D

Explanation:

The best course of action for the CIO is to develop and communicate an accountability matrix. An accountability matrix, also known as a responsibility assignment matrix, is a project management tool that defines the roles and responsibilities of different stakeholders in a project or process1 An accountability matrix can help to clarify who is responsible, accountable, consulted, and informed (RACI) for each task or deliverable, and avoid confusion and ambiguity in the decision-making process2 By developing and communicating an accountability matrix, the CIO can ensure that the IT portfolio management policies and processes are understood and followed by all the relevant parties, and that the IT projects are aligned with the enterprise goals. Reference: RACI Matrix: Responsibility Assignment Matrix Guide 20233, Responsibility assignment matrix - Wikipedia2, Accountability Matrix - Explained - The Business Professor, LLC1

Question: 106

Which of the following responsibilities should be retained within an enterprise when outsourcing a project management office (PMO) function?

A. Selecting projects
B. Managing projects
C. Tracking project cost
D. Defining project methodology

Answer: A

Explanation:

The responsibility that should be retained within an enterprise when outsourcing a project management office

(PMO) function is selecting projects. This is because selecting projects is a strategic decision that involves aligning the project portfolio with the enterprise goals, vision, and mission. Selecting projects also requires understanding the business needs, priorities, and value proposition of each project, as well as the available resources, risks, and opportunities. These are aspects that the enterprise should have more knowledge and authority over than theoutsourced PMO provider. Outsourcing the project selection process may result in a loss of control, alignment, and accountability for the enterprise. Therefore, selecting projects is a responsibility that should be retained within an enterprise when outsourcing a PMO function.

Reference: Build the Next Gen PMO by Outsourcing - Project Management Institute1, How to Outsource a PMO: Your Options and Which Will Suit Your Business - PM Majik2, What is an Outsourced PMO and How Does it Work? - PM Majik3

Question: 107

Which of the following should be the MOST important consideration when defining an information architecture?

A. Frequency and quantity of information updates
B. Information to justify business cases
C. Incorporation of emerging technologies
D. Access to and exchange of information

Answer: D

Explanation:

The most important consideration when defining an information architecture is access to and exchange of information. Information architecture (IA) is the process of guiding users through the site by organising and arranging all the relevant content in a clear, intuitive way1. The main purpose of IA is to help users find information and complete tasks2. To do this, IA needs to consider how users
access and exchange information within the digital product or service, and how to make it easy, fast, and satisfying for them. Access to and exchange of information involves aspects such as:

Navigation systems: How users browse or move through information2. Navigation systems should be consistent, predictable, and visible, and should provide feedback and orientation cues to the users3. Search systems: How users look for information2. Search systems should be accurate, relevant, and comprehensive, and should support different types of queries and filters4.

Labelling systems: How information is represented and classified2. Labelling systems should use clear, concise, and meaningful words that match the users' expectations and vocabulary.

Information structure: How information is organised into categories, hierarchies, and relationships2. Information structure should reflect the users' mental models and tasks, and should avoid unnecessary complexity or ambiguity.

By considering access to and exchange of information when defining an IA, the organization can ensure that the information assets are usable, findable, and accessible to the users, and that they support the user experience and the business goals. Reference: Information Architecture Basics | Usability.gov1, What is information architecture? - UX Design Institute2, Navigation Design Basics: Tips & Best Practices - Adobe XD Ideas3, Search System Design: Best Practices & Tips- Adobe XD Ideas4, Labeling Systems: An Introduction to Information Architecture - Boxes …, Information Architecture 101: Techniques and Best Practices - Adobe …

Question: 108

Which of the following roles has PRIMARY accountability for the security related to data assets?

A. Database administrator
B. Data owner
C. Data analyst

D. Security architect

Answer: B

Explanation:

The role that has primary accountability for the security related to data assets is the data owner. A data owner is a person who is generally in a senior company position, responsible for the categorization, protection, usage, and quality of one or more data sets1. The data owner must ensure that the information within their domain is correctly maintained across various platforms and business processes, and that it is secured from unauthorized access and misuse2. The data owner also has the authority to grant or revoke access rights to the data, and to define and enforce data security policies and standards3. Therefore, the data owner is the primary accountable role for the security related to data assets. Reference: Data Owners vs. Data Stewards vs. Data Custodians - CPO Magazine2, CISSP domain 2: Asset security - Infosec Resources

Question: 109

Senior management is reviewing the results of a recent security incident with significant business impact. Which of the following findings should be of GREATEST concern?

A. Significant gaps are present m the incident documentation.
B. The incident was not logged in the ticketing system.
C. Response decisions were made without consulting the appropriate authority.
D. Response efforts had to be outsourced due to insufficient internal resources.

Answer: C

Explanation:

The finding that should be of greatest concern to senior management is that response decisions were made without consulting the appropriate authority. This is because response decisions are critical actions that can affect the outcome and impact of a security incident, and they should be made by the designated authority who has the responsibility and accountability for the incident response. According to CISA, the Department of Justice, through the FBI and the NCIJTF, is thelead agency for threat response during a significant incident, with DHS's investigative agencies—the Secret Service and ICE/HSI - playing a crucial role in criminal investigations1. If response decisions are made without consulting the appropriate authority, it may result in:

Legal or regulatory violations: The response actions may not comply with the applicable laws or regulations, such as data breach notification, evidence preservation, or privacy protection. This may expose the organization to legal or regulatory penalties, lawsuits, or reputational damage.

Ineffective or counterproductive actions: The response actions may not be aligned with the incident response plan, best practices, or standard operating procedures. This may cause more harm than good, such as escalating the incident, destroying evidence, or compromising recovery efforts.

Lack of coordination and communication: The response actions may not be coordinated or communicated with the relevant stakeholders, such as senior management, legal counsel, public relations, or external partners. This may lead to confusion, inconsistency, or mistrust among the parties involved in the incident response.

Therefore, senior management should be most concerned about the finding that response decisions were made without consulting the appropriate authority, and they should take corrective actions to prevent this from happening again in the future. Reference: Cybersecurity Incident Response | CISA1

Question: 110

A large enterprise that is diversifying its business will be transitioning to a new software platform, which is expected to cause data changes. Which of the following should be done FIRST when developing the related metadata management process?

A. Require an update to enterprise data policies.
B. Request an impact analysis.
C. Review documented data interdependence.
D. Validate against existing architecture.

Answer: B

Explanation:

The first thing that should be done when developing the metadata management process for the new software platform is to request an impact analysis. An impact analysis is a process of assessing the potential effects of a change on the existing system, processes, and stakeholders1. An impact analysis can help to identify the following aspects2:

The scope and objectives of the change: What are the expected benefits and outcomes of the new software platform? How does it align with the enterprise strategy and goals?

The current state and baseline: What are the existing data sources, formats, standards, and quality levels? How are they documented, stored, and accessed? Who are the data owners, stewards, and users?

The gaps and risks: What are the data changes that will occur due to the new software platform? How will they affect the data quality, security, privacy, and compliance? What are the potential challenges or issues that may arise during or after the transition?

The mitigation and contingency plans: How can the data changes be minimized or avoided? How can the data quality, security, privacy, and compliance be ensured or improved? What are the alternative solutions or fallback options in case of failure or disruption?

By requesting an impact analysis, the organization can gain a better understanding of the data environment and the implications of the new software platform. This can help to develop a metadata management process that is consistent, effective, and adaptable to the change. Reference: Impact Analysis: A Key Aspect of Preventing Problems | Project …1, Impact Analysis: The Key to Successful Change Management2

Question: 111

An IT director has become aware that a certain subset of data collected lawfully can be used to generate additional revenue. However, this particular use of the data is outside the original intention. What is the PRIMARY reason this situation should be escalated to the IT steering committee?

A. Potential legal penalties
B. Ethical concerns
C. Regulatory requirements
D. Data protection

Answer: B

Explanation:

The primary reason this situation should be escalated to the IT steering committee is B. Ethical concerns. This is because using data for a purpose that is outside the original intention may violate the principle of purpose limitation, which states that personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes1. Using data for a different purpose may also breach the trust and expectations of the individuals who provided the data, and may harm their rights and interests. Therefore, the IT director should consult the IT steering committee, which is a group of senior executives who are responsible for developing and enforcing the organization's IT priorities and policies2, to determine whether the new use of data is ethical, lawful, and transparent. The IT steering committee should also consider the following aspects before making a decision:

The link between the original purpose and the new/upcoming purpose: How closely related are the two purposes? Is the new purpose compatible with the original purpose or does it contradict it? The context in which the data was collected: What was the relationship between the organization and the individuals at the time of data collection? What did the individuals consent to or expect from the data processing?
The type and nature of the data: Is the data sensitive, personal, or confidential? Does it reveal any information about the individuals' identity, preferences, behavior, or opinions?
The possible consequences of the intended further processing: How will the new use of data affect the individuals and the organization? Will it benefit or harm them? Will it create any risks or opportunities?
The existence of appropriate safeguards: What measures are in place to protect and manage the data according to the data protection principles and standards? How can the data quality, security, privacy, and compliance be ensured or improved?
By escalating this situation to the IT steering committee, the IT director can ensure that the ethical implications of using data for another purpose are properly assessed and addressed.

Question: 112

Of the following, who should approve the criteria for information quality within an enterprise?

A. Information architect
B. Information analyst
C. Information steward
D. Information owner

Answer: D

Explanation:

Information owners are responsible for defining the quality criteria for information within their domain, based on business requirements and stakeholder expectations. Information owners are also accountable for ensuring that information quality is maintained and improved. Reference := COBIT 5: Enabling Information, chapter 4, section 4.2.1

Question: 113

From a governance perspective, the PRIMARY goal of an IT risk optimization process should be to ensure:

A. IT risk thresholds are defined in the enterprise architecture (EA).
B. the IT risk mitigation strategy is approved by management.
C. IT risk is mapped to the balanced scorecard.
D. the impact of IT risk to the enterprise is managed.

Answer: D

Explanation:

The primary goal of an IT risk optimization process from a governance perspective is to ensure that the impact of IT risk to the enterprise is managed in alignment with the enterprise risk management (ERM) framework and the enterprise objectives. IT risk optimization is not only about defining thresholds, approving strategies or mapping metrics, but about ensuring that IT risk is effectively mitigated, monitored and communicated to support the achievement of enterprise goals. Reference := CGEIT Exam Content Outline, Domain 4: Risk Optimization1; Certified in Governance of Enterprise IT (CGEIT) Course, Learning Tree2

Question: 114

Which of the following is the BEST way to ensure new systems can be adequately supported once in

production?

A. Establish a resource management framework.
B. Evaluate the operational requirements of the business stakeholders.
C. Identify key performance indicators (KPIs).
D. Require operational management be identified in the business case.

Answer: D

Explanation:

The best way to ensure new systems can be adequately supported once in production is to require operational management be identified in the business case. This means that the business case should include the costs, benefits, risks and resources associated with the operation and maintenance of the new system, as well as the roles and responsibilities of the operational staff. By doing so, the business case can ensure that the new system is aligned with the business objectives and can deliver value to the stakeholders. Additionally, the business case can help to secure the commitment and support of the operational management for the new system. Reference := CGEIT Exam Content Outline, Domain 3: Benefits Realization1; COBIT 5: Enabling Processes, chapter 4, section 4.2.22; Building A Governance System: A Review of Information Flow and Items Component

Question: 115

To benefit from economies of scale, a CIO is deciding whether to outsource some IT services. Which of the following would be the MOST important consideration during the decision-making process?

A. IT staff morale
B. Core IT processes
C. Outsourcer's reputation
D. New service level agreements (SLAs)

Answer: B

Explanation:

The most important consideration during the decision-making process of outsourcing some IT services is to identify the core IT processes that are critical for the organization’s strategic objectives and competitive advantage. Core IT processes are those that provide unique value to the organization and differentiate it from its competitors. Outsourcing core IT processes may result in loss of control, innovation, and differentiation, as well as increased dependency and risk. Therefore, core IT processes should be retained in-house, while non-core IT processes can be outsourced to benefit from economies of scale, cost reduction, and access to specialized skills and technologies. Reference := CGEIT Exam Content Outline, Domain 3: Benefits Realization1; COBIT 5: Enabling Processes, chapter 4, section 4.2.32; IT governance -managing the outsourcing relationship

Question: 116

The board and senior management of a new enterprise recently met to formalize an IT governance framework. The board of directors' FIRST step in implementing IT governance is to ensure that: A. an IT balanced scorecard is implemented.

B. a portfolio of IT-enabled investments is developed.
C. IT roles and responsibilities are established.
D. IT policies and procedures are defined.

Answer: C

Explanation:

The first step in implementing IT governance is to ensure that IT roles and responsibilities are established. This means that the board of directors should define the authority, accountability, and decision rights of the key stakeholders involved in IT governance, such as the board itself, senior management, business units, IT function, and external parties. By doing so, the board can ensure

that IT governance is aligned with the enterprise governance and strategy, and that IT performance and value delivery are monitored and evaluated. Establishing IT roles and responsibilities is also a prerequisite for defining IT policies and procedures, developing a portfolio of IT-enabled investments, and implementing an IT balanced scorecard. Reference := CGEIT Exam Content Outline, Domain 1: Framework for the Governance of Enterprise IT1; COBIT 5: Enabling Processes, chapter 4, section 4.1.12; Improve IT Governance to Drive Business Results

Question: 117

An IT risk assessment for a large healthcare group revealed an increased risk of unauthorized disclosure of information. Which of the following should be established FIRST to address the risk?

A. Data encryption tools
B. Data loss prevention tools
C. Data classification policy
D. Data retention policy

Answer: C

Explanation:

The first step to address the risk of unauthorized disclosure of information is to establish a data classification policy. A data classification policy defines the categories of data based on their sensitivity and value to the organization, and specifies the appropriate security controls and handling procedures for each category. A data classification policy helps to identify the most critical and confidential data, and to prioritize the protection of such data from unauthorized access, disclosure, modification, or loss. A data classification policy also provides a basis for implementing other measures, such as data encryption tools, data loss prevention tools, and data retention policy, to enhance the security of data. Reference := Reducing Cybersecurity Security Risk From and to Third Parties; Unauthorized Access: Prevention Best Practices; Security of Enterprise Application Integration

Question: 118

Which of the following should be the MAIN governance focus when implementing a newly approved bring your own device (BYOD) policy?

A. Recommending mobile applications that will increase business productivity
B. Training employees on the enterprise's chosen mobile device management system
C. Educating employees on the increased IT security risk to the enterprise
D. Understanding knowledge gaps of IT employees to support different mobile platforms

Answer: C

Explanation:

The main governance focus when implementing a newly approved BYOD policy is to educate employees on the increased IT security risk to the enterprise. BYOD introduces various challenges and threats to the enterprise's data and network security, such as device loss or theft, unauthorized access, malware infection, data leakage, and compliance violations. Therefore, it is essential to raise the awareness and understanding of employees on the potential risks and their responsibilities in protecting the enterprise's assets and information. Educating

Watermark Sample

employees on the IT security risk can also help to foster a culture of security and compliance, and to promote best practices for BYOD
usage, such as following the acceptable use policy, installing security software, and reporting incidents.
Reference := The Ultimate Guide to BYOD Security: Definition & More - Digital Guardian; Enterprise mobility and security: How to build a BYOD policy; Bring Your Own Device for Executives | Cyber.gov.au

Question: 119

An audit report has revealed that data scientists are analyzing sensitive "big data" files using an offsite cloud because corporate servers do not have the necessary processing capabilities. A review of policies indicates this practice is not prohibited. Which of the following should be the FIRST strategic action to address the report?

A. Authorize a risk analysis of the practice.
B. Update data governance practices.
C. Revise the information security policy.
D. Recommend the use of a private cloud.

Answer: A

Explanation:

The first strategic action to address the report is to authorize a risk analysis of the practice. A risk analysis is a systematic process of identifying, assessing, and prioritizing the potential threats and vulnerabilities that may arise from the use of an offsite cloud for analyzing sensitive “big data” files. A risk analysis can help to determine the level of exposure and impact of the practice on the organization’s data security, privacy, compliance, and performance. A risk analysis can also provide recommendations for mitigating or avoiding the risks, such as implementing appropriate controls, policies, and procedures.
Updating data governance practices, revising the information security policy, and recommending the use of a private cloud are possible actions that may result from the risk analysis, but they are not the first step. Data governance practices are the rules and processes that define how data is created, stored, accessed, used, and disposed of within an organization. Data governance practices should align with the organization’s data strategy, objectives, and values. Information security policy is a document that outlines the principles, guidelines, and responsibilities for protecting the confidentiality, integrity, and availability of data. Information security policy should reflect the organization’s risk appetite, legal obligations, and industry standards. A private cloud is a cloud computing model that provides dedicated resources and services to a single organization. A private cloud may offer more control, security, and customization than an offsite cloud, but it may also require more investment, maintenance, and expertise.
Therefore, before updating data governance practices, revising the information security policy, or recommending the use of a private cloud, it is important to conduct a risk analysis of the current practice of using an offsite cloud for analyzing sensitive “big data” files. This will help to ensure that the organization makes informed and strategic decisions that balance the benefits and risks of using cloud computing for big data analytics.

Question: 120

Which of the following BEST lowers costs and improves scalability from an IT enterprise architecture (EA) perspective?

A. Cost management
B. IT strategic sourcing
C. Standardization
D. Business agility

Answer: C

Explanation:

Standardization is the best option to lower costs and improve scalability from an IT enterprise architecture perspective, because it reduces complexity, increases interoperability, and enables reuse of IT resources. Reference:= ISACA, CGEIT Review Manual, 27th Edition, 2019, page 79.

Question: 121

While assessing the feasibility of introducing new IT practices and standards into the IT governance framework, it is CRITICAL to understand an organization's:

A. culture.
B. level of outsourcing.
C. enterprise architecture (EA).
D. maturity of IT processes.

Answer: A

Explanation:

Culture is the most critical factor to understand while assessing the feasibility of introducing new IT practices and standards into the IT governance framework, because it influences the behavior, values, and beliefs of the organization and its stakeholders. Culture affects how IT governance is perceived, implemented, and evaluated in the organization. A mismatch between the organizational culture and the IT governance framework can lead to resistance, conflict, and poor performance. Therefore, it is essential to assess the current culture of the organization and its readiness for change before introducing new IT practices and standards. Reference := The Influence of Organizational Culture in Application of Information Technology Governance, The Value of IT Governance, Organisational Governance Explained: The Keys to Success

Question: 122

When determining the optimal IT service levels to support business, which of the following is MOST important?

A. IT capacity utilization and availability.
B. Cost/benefit to the business.
C. Available IT budget.
D. Business user requests

Answer: B

Explanation:

When determining the optimal IT service levels to support business, the most important factor is the cost/benefit to the business. This means that the IT service levels should be aligned with the business objectives, needs, and expectations, and that the benefits of providing a certain level of IT service should outweigh the costs of delivering it. The cost/benefit analysis should consider both the direct and indirect costs and benefits of IT service levels, such as the impact on customer satisfaction, revenue, productivity, quality, risk, compliance, innovation, and competitive advantage. A cost/benefit analysis can help IT managers justify their IT service level decisions and communicate them effectively to the business stakeholders. Reference := IT cost/benefit analysis: Why it matters and how to do it right, IT Support Levels Clearly Explained: L1, L2, L3 & More, IT support levels: definition, tiers and advantages, The Importance of Adopting Formal IT Service Management

Question: 123

Which of the following is MOST important when an IT-enabled business initiative involves multiple business functions?

A. Defining cross-departmental budget allocation
B. Conducting a systemic risk assessment
C. Developing independent business cases
D. Establishing a steering committee with business representation

Answer: D

Explanation:

Establishing a steering committee with business representation is the most important factor when an IT-enabled business initiative involves multiple business functions, because it ensures that the initiative is aligned with the strategic goals and needs of the organization, and that the different business functions have a voice and a stake in the decision-making process. A steering committee can also provide guidance, support, and oversight to the IT team and help resolve any conflicts or issues that may arise among the business functions. A steering committee can also monitor the progress and performance of the initiative and ensure that it delivers the expected benefits and value to the organization. Reference := What is an IT Steering Committee? – BMC Software | Blogs, Steering Committee: Definition, Roles & Meeting Tips - ProjectManager, How To Create an IT Steering Committee in 6 Steps - Indeed

Question: 124

A recent benchmarking analysis has indicated an IT organization is retaining more data and spending significantly more on data retention than its competitors. Which of the following would BEST ensure the optimization of retention costs?

A. Requiring that all business cases contain data deletion and retention plans
B. Revalidating the organization's risk tolerance and re-aligning the retention policy
C. Moving all high-risk and medium-risk data backups to cloud storage
D. Redefining the retention policy to align with industry best practices

Answer: B

Explanation:

Revalidating the organization’s risk tolerance and re-aligning the retention policy is the best option to ensure the optimization of retention costs, because it can help the organization balance the trade-off between the benefits and costs of data retention. By revalidating the risk tolerance, the organization can identify the optimal level of data retention that minimizes the exposure to legal, regulatory, and operational risks, while also reducing the storage and management costs. By re-aligning the retention policy, the organization can ensure that the data retention practices are consistent with the risk tolerance and reflect the current business needs and objectives. A re-aligned retention policy can
also help the organization comply with data retention laws and regulations, avoid unnecessary data hoarding, and improve data quality and accessibility. Reference := Data Retention Policy 101: Best Practices, Examples & More - Intradyn, Data Retention 101: Policies and Best Practices | Egnyte, Best Practices for Data Retention and Policy Creation Will Optimize Storage Management, Data Retention Policy: Crafting Strategy for Compliance and Access

Question: 125

Which of the following MOST effectively prevents an IT system from becoming technologically obsolete

before its planned return on investment (ROi)?

A. Requesting periodic third-party assessments of the system throughout its life
B. Obtaining long-term support commitments from the system platform vendors)
C. Obtaining independent assurance that the system will conform to future business requirements
D. Ensuring that the system is maintained in compliance with enterprise architecture (EA) standards

Answer: D

Explanation:

Ensuring that the system is maintained in compliance with enterprise architecture (EA) standards is the most effective way to prevent an IT system from becoming technologically obsolete before its planned return on investment (ROI), because it ensures that the system is aligned with the current and future business needs, goals, and strategies of the organization. Enterprise architecture (EA) standards define the principles, guidelines, and best practices for designing, developing, and managing IT systems in a consistent, coherent, and integrated manner across the organization. By following EA standards, IT leaders can ensure that the system is compatible with the existing and emerging technologies, platforms, and frameworks that support the business processes and functions. EA standards also help IT leaders to monitor and evaluate the performance, quality, security, and reliability of the system, and to identify and address anygaps, issues, or risks that may affect its functionality or value. EA standards also facilitate the communication and collaboration among different stakeholders involved in the system lifecycle, such as business users, IT staff, vendors, and auditors. By maintaining the system in compliance with EA standards, IT leaders can ensure that the system delivers the expected benefits and value to the organization and achieves its planned ROI. Reference := ISO/IEC/IEEE 42020:2019(en), Software, systems and enterprise ?

Architecture processes, Sample: Enterprise Architecture Standards - CIO Portal, Obsolescence management for IT leaders - Information Age

Question: 126

The board of a start-up company has directed the CIO to develop a technology resource acquisition and management policy. Which of the following should be the MOST important consideration during the development of this policy?

A. Enterprise growth plans
B. Industry best practices
C. Organizational knowledge retention
D. IT staff competencies

Answer: A

Explanation:

Enterprise growth plans should be the most important consideration during the development of a technology resource acquisition and management policy, because they define the vision, goals, and strategies of the start-up company and how technology can support them. A technology resource acquisition and management policy should align with the enterprise growth plans and ensure that the technology resources are acquired and managed in a way that enables the company to achieve its desired outcomes, such as increasing market share, enhancing customer satisfaction, improving operational efficiency, or creating innovative products or services. A technology resource acquisition and management policy should also consider the scalability, flexibility, and adaptability of the technology resources to accommodate the changing needs and demands of the company as it grows and evolves. A technology resource acquisition and management policy should also balance the costs and benefits of acquiring and managing technology resources and ensure that they deliver value to the company and its stakeholders.

Reference := Managing Technology as a Business Strategy, A Complete Guide To Strategic Technology Planning, Policy on IT Acquisition Strategies and Planning Under FITARA

Question: 127

When developing effective metrics for the measurement of solution delivery, it is MOST important to:

A. establish project controls and monitoring objectives.
B. perform an objective analysis of the project roadmap.
C. establish the objectives and expected benefits.
D. specify quantitative measures for solution delivery.

Answer: C

Explanation:

Establishing the objectives and expected benefits is the most important step when developing effective metrics for the measurement of solution delivery, because it defines the purpose, scope, and value of the solution and how it aligns with the business goals and needs. By establishing the objectives and expected benefits, IT leaders can identify the key performance indicators (KPIs) that will measure the progress, quality, and outcomes of the solution delivery. KPIs are specific, measurable, achievable, relevant, and time-bound metrics that track and evaluate the performance of the solution delivery against the objectives and expected benefits. KPIs can also help IT leaders to communicate the value proposition of the solution to the stakeholders, monitor and manage the risks and issues that may affect the solution delivery, and ensure that the solution meets or exceeds the expectations of the customers and users. Reference := Automation: metrics that measure success, 4 Types of Key Performance Metrics To Track (With Examples), A guide to measuring benefits effectively

Question: 128

Which of the following is the BEST indication of effective IT-business strategic alignment?

A. Business management is involved as IT strategies are developed.
B. IT senior management is required to report to the board.
C. Business strategy is documented to allow IT architecture to be designed quickly.
D. IT-business collaboration results in a strategy focused on IT cost reduction.

Answer: A

Explanation:

Business management involvement as IT strategies are developed is the best indication of effective IT-business strategic alignment, because it ensures that the IT strategies are aligned with the business goals, needs, and expectations, and that the business stakeholders have a clear understanding and ownership of the IT initiatives. Business management involvement can also facilitate the communication, collaboration, and coordination between the IT and business functions, and help resolve any conflicts or issues that may arise during the IT strategy development process. Business management involvement can also foster a culture of trust, mutual respect, and shared vision between the IT and business functions, and enhance the value proposition and performance of the IT strategies. Reference := IT Strategic Planning and Alignment: Best Practices, What Is "IT-Business Alignment"?, Aligning IT and Business Strategy for Project Success

Question: 129

The BEST way to manage an outsourced vendor relationship is by:

A. conducting periodic risk assessments.
B. reviewing annual independent third-party reports.
C. providing clear objectives and transparency.

D. analyzing performance statistics from the vendor.

Answer: C

Explanation:

Providing clear objectives and transparency is the best way to manage an outsourced vendor relationship, because it ensures that both parties have a common understanding of the expectations, deliverables, and outcomes of the outsourcing arrangement. By providing clear objectives, the client can communicate the business goals, needs, and requirements to the vendor, and the vendor can align their services, processes, and resources accordingly. By providing transparency, the client can share relevant information, feedback, and insights with the vendor, and the vendor can report on their performance, issues, and risks regularly. Providing clear objectives and transparency can also foster trust, collaboration, and innovation between the client and the vendor, and help resolve any conflicts or disputes that may arise. According to Outsourcing Vendor Best Practices: 5 Tips for a Successful Relationship, "Transparency is critical to a successful outsourcing relationship. It helps to ensure that both parties are on the same page regarding expectations, deliverables and performance."

Question: 130

Which of the following BEST reflects mature risk management in an enterprise?

A. A regularly updated risk register
B. Ongoing risk assessment
C. Ongoing investment in risk mitigation
D. Responsive risk awareness culture

Answer: D

Explanation:

A responsive risk awareness culture is the best reflection of mature risk management in an enterprise, because it implies that the organization has a high level of risk maturity that enables it to reduce noise and focus more effectively on truly high-risk concerns, choose cost-effective solutions for the risk management priorities, and execute reliably1. A responsive risk awareness culture also means that the organization has a clear and consistent risk appetite and tolerance, and that the employees are cognizant of the relevant risks as part of their actions2. A responsive risk awareness culture also fosters trust, collaboration, and innovation among the stakeholders, and helps the organization to adapt to changing business environments and emerging risks3.

The other options are not as indicative of mature risk management in an enterprise, because they are either too narrow or too reactive. A regularly updated risk register is a useful tool forcataloguing, tracking, and mitigating risks, but it does not necessarily reflect the strategic alignment, integration, or performance of the risk management process4. Ongoing risk assessment is an essential activity for identifying and evaluating risks, but it does not guarantee that the risks are prioritized, communicated, or managed effectively5. Ongoing investment in risk mitigation is a sign of commitment to risk management, but it does not ensure that the investment is aligned with the risk appetite and tolerance, or that it delivers value to the organization5.

Question: 131

An enterprise is initiating efforts to improve system availability to mitigate IT risk to the business.
Which of the following results would be MOST important to report to the CIO to measure progress?

A. Incident severity and downtime trend analysis
B. Probability and seventy of each IT risk

C. Financial losses and bad press releases
D. Customer and stakeholder complaints over time

Answer: A

Explanation:

Incident severity and downtime trend analysis is the most important result to report to the CIO to measure progress in improving system availability to mitigate IT risk to the business, because it directly reflects the impact and frequency of system failures or disruptions on the business operations, processes, and functions. By analyzing the severity and duration of incidents over time, the CIO can evaluate the effectiveness of the IT risk management and system availability strategies, and identify any gaps, issues, or opportunities for improvement. Incident severity and downtime trend analysis can also help the CIO to communicate the value and performance of the IT risk management and system availability initiatives to the business stakeholders, and justify any further investment or action required to achieve the desired outcomes.
The other options are not as important as incident severity and downtime trend analysis, because they are either too indirect or too subjective to measure progress in improving system availability to mitigate IT risk to the business. Probability and severity of each IT risk is a useful input for IT risk management, but it does not necessarily reflect the actual occurrence or impact of system failures or disruptions on the business1. Financial losses and bad press releases are possible consequences of system failures or disruptions, but they may not capture the full extent or root causes of the IT risk to the business2. Customer and stakeholder complaints over time are indicators of customer satisfaction and loyalty, but they may not be reliable or consistent measures of system availability or IT risk to the business

Question: 132

A review of the effectiveness of IT governance within an enterprise has revealed that several innovation improvement initiatives are failing. An analysis shows a lack of stakeholder buy-in to the improvements. Implementing which of the following would have prevented this problem?

A. An IT project roadmap
B. An IT risk management program
C. A change management program
D. A service delivery framework

Answer: C

Explanation:

A change management program is the best option to prevent the problem of a lack of stakeholder buy-in to the innovation improvement initiatives, because it is a systematic and structured approach to managing the human side of change and ensuring that the stakeholders are engaged, informed, and committed to the change process. A change management program can help to identify and analyze the stakeholders, their needs, expectations, and concerns, and develop appropriate strategies and actions to communicate, educate, involve, and support them throughout the change journey. A change management program can also help to assess and address the potential risks, barriers, and resistance to change, and monitor and measure the effectiveness and outcomes of the change initiatives. According to Making Change Happen: 5 Keys to Driving Successful Change Initiatives, “Stakeholders are all the people who affect or are affected by the change initiative. Project participants can’t make the change happen by themselves. They need champions and supporters. It’s important to align stakeholders around the overall vision and then actively engage them throughout the process.”

Question: 133

Which of the following is the BEST way for a CIO to secure support for a strategy to achieve long-term IT objectives?

A. Make the necessary strategic decisions and notify staff accordingly.
B. Develop tactics to implement the strategy and share with stakeholders.
C. Develop a communication plan for distribution of information to staff.
D. Meet with stakeholders to explain the strategy and incorporate feedback.

Answer: D

Explanation:

Meeting with stakeholders to explain the strategy and incorporate feedback is the best way for a CIO to secure support for a strategy to achieve long-term IT objectives, because it ensures that the strategy is aligned with the needs, expectations, and interests of the stakeholders, and that the stakeholders are engaged, informed, and committed to the strategy. By meeting with stakeholders, the CIO can communicate the vision, goals, and benefits of the strategy, andaddress any questions, concerns, or objections that the stakeholders may have. By incorporating feedback, the CIO can demonstrate respect and appreciation for the stakeholder input, and make any necessary adjustments or improvements to the strategy based on the stakeholder perspectives. Meeting with stakeholders and incorporating feedback can also foster trust, collaboration, and innovation between the CIO and the stakeholders, and enhance the value proposition and performance of the strategy. The other options are not as effective as meeting with stakeholders and incorporating feedback, because they are either too autocratic, too vague, or too passive to secure support for a strategy to achieve long-term IT objectives. Making the necessary strategic decisions and notifying staff accordingly is a top-down approach that may alienate or antagonize the stakeholders, and create resistance or conflict. Developing tactics to implement the strategy and share with stakeholders is a tactical approach that may not address the strategic alignment, integration, or evaluation of the strategy. Developing a communication plan for distribution of information to staff is a one-way approach that may not elicit stakeholder feedback, engagement, or commitment. According to Stakeholder management: Your plan for influencing project outcomes, "Stakeholder management is essentially stakeholder relationship management as it is the relationship and not the actual stakeholder groups that are managed."

Question: 134

Two large financial institutions with different corporate cultures are engaged in a merger. From a governance perspective, which of the following should be the GREATEST concern?

A. Technology infrastructure
B. Risk appetite
C. Combined cost of operations
D. Enterprise architecture (EA) integration

Answer: B

Explanation:

Risk appetite is the greatest concern from a governance perspective when two large financial institutions with different corporate cultures are engaged in a merger, because it reflects the amount and type of risk that the organizations are willing to pursue, retain, or take in order to achieve their strategic objectives. Risk appetite is influenced by various factors, such as organizational culture, values, beliefs, and behaviors, as well as external factors, such as market conditions, regulations, and stakeholder expectations. Therefore, if the two merging organizations have different risk appetites, this may create challenges and conflicts in aligning their strategies, policies, processes, and systems. It may also affect their performance, compliance, reputation, and value

creation. Therefore, it is important to assess and harmonize the risk appetites of the two organizations and ensure that they are consistent with their merged vision, goals, and needs. Reference := Good Governance Institute Board guidance on riskappetite, Risk Appetite: A Conversation of Governance, Organisations must define their IT risk appetite and tolerance

Question: 135

A healthcare enterprise that is subject to strict compliance requirements has decided to outsource several key IT services to third-party providers. Which of the following would be the BEST way to assess compliance and avoid reputational damage?

A. Require quarterly reports from the providers demonstrating compliance.
B. Require documentation that the providers have adequate controls in place.
C. Exercise the right to perform an audit.
D. Impose monetary penalties for noncompliance.

Answer: C

Explanation:

Exercising the right to perform an audit is the best way to assess compliance and avoid reputational damage when outsourcing key IT services to third-party providers, especially in a highly regulated industry like healthcare. An audit is a systematic and independent examination of the provider's policies, procedures, controls, and performance related to the outsourced IT services, and it can help to verify that the provider is complying with the contractual obligations, service level agreements, and regulatory requirements. An audit can also help to identify and address any gaps, issues, or risks that may affect the quality, security, or reliability of the outsourced IT services, and to ensure that the provider is delivering value and meeting the expectations of the enterprise. An audit can also provide assurance and confidence to the enterprise's senior management, board, and stakeholders that the outsourcing arrangement is effective, efficient, and compliant. According to Outsourcing Compliance: What You Need to Know, "The right to audit clause should be included in every contract with a third- party service provider. It allows the organization to conduct an independent review of the provider's compliance with applicable laws and regulations, contractual terms and conditions, and industry standards and best practices."

Question: 136

An enterprise plans to expand into new markets in countries lacking data privacy regulations, increasing risk exposure. Which of the following is the BEST course of action for the CIO?

A. Identify business risk appetite and tolerance levels.
B. Quantify the risk impact and evaluate possible countermeasures.
C. Limit the personal data available to the high-risk countries.
D. Mandate the strengthening of user access controls.

Answer: A

Explanation:

The best course of action for the CIO in this scenario is to identify business risk appetite and tolerance levels. Risk appetite is the amount and type of risk that an organization is willing to pursue, retain, or take in order to achieve its strategic objectives. Risk tolerance is the acceptable level of variation from the risk appetite. By identifying the business risk appetite and tolerance levels, the CIO can align the IT strategy and operations with the business goals, needs, and expectations, and ensure that the IT risks are managed within the acceptable boundaries. Identifying the business risk appetite and tolerance levels can also help the CIO to communicate and justify the IT decisions and actions to the senior management, board, and stakeholders, and to balance the costs and benefits of IT investments and initiatives. According to CPG 235 – Managing Data Risk, "The adequacy

of data controls in ensuring that a regulated entity operates within its risk appetite would normally be assessed as part of introducing new business processes and then on a regular basis thereafter (or following material change to either the process, usage of data, internal controls or external environments)."

Question: 137

A global financial institution has decided to integrate data from branch locations into a common database to address regulatory reporting requirements. Analysis of data flows and the full data life cycle should be conducted at which level?

A. Transaction level
B. Enterprise level
C. Branch level
D. Department level

Answer: B

Explanation:

Analysis of data flows and the full data life cycle should be conducted at the enterprise level, because it provides a holistic and comprehensive view of how data is created, stored, processed, used, and disposed of across the entire organization. By conducting data analysis at the enterprise level, the financial institution can ensure that the data integration from branch locations is aligned with the business objectives, needs, and expectations, and that the data quality, security, and compliance are maintained throughout the data life cycle. Data analysis at the enterprise level can also help to identify and address any data gaps, issues, or risks that may affect the regulatory reporting requirements or the performance and value of the data. According to Data Life Cycle and Data Governance What CDOs and CISOs Can Learn, "Data governance is an enterprise-wide program that requires a holistic approach to managing data throughout its life cycle."

Question: 138

An enterprise's service center is experiencing long delays in fulfilling! T service requests and very low customer satisfaction. The BEST way to determine if staff competency is the root cause of these performance problems is to compare required staff competencies with:

A. certification requirements.
B. current skills inventory.
C. training program completions.
D. hiring and staffing practices.

Answer: B

Explanation:

The best way to determine if staff competency is the root cause of the performance problems is to compare the required staff competencies with the current skills inventory of the service center staff. This will help identify any gaps or mismatches between what is expected and what is available in terms of skills and knowledge. Reference: CGEIT Review Manual, 7th Edition, page 113.

Question: 139

Which of the following are PRIMARY factors in ensuring the success of an enterprise quality assurance program?

A. Enterprise risk appetite and tolerance
B. Risk management and control frameworks

C. Continuous improvement plans
D. A process maturity framework and documented procedures

Answer: D

Explanation:

A process maturity framework and documented procedures are primary factors in ensuring the success of an enterprise quality assurance program because they provide a clear and consistent way of measuring, monitoring, and improving the quality of the processes and products. A process maturity framework, such as the Capability Maturity Model Integration (CMMI), defines the levels of maturity and the best practices for each level. Documented procedures, such as standard operating procedures (SOPs), define the steps, roles, responsibilities, and tools for each process. These factors help to ensure that the quality assurance program is aligned with the business objectives, customer expectations, and industry standards.

Question: 140

Which of the following is the BEST way to demonstrate that IT strategy supports a new enterprise strategy?

A. Monitor new key risk indicators (KRIs).
B. Measure return on IT investments against balanced scorecards.
C. Review and update the portfolio management process.
D. Map IT programs to business goals.

Answer: D

Explanation:

The best way to demonstrate that IT strategy supports a new enterprise strategy is to map IT programs to business goals. This will show how IT initiatives are aligned with and contribute to the achievement of the enterprise vision, mission, and objectives. Mapping IT programs to business goals will also help to prioritize, monitor, and evaluate the performance and value of IT investments

Question: 141

Prior to setting IT objectives, an enterprise MUST have established its:

A. architecture.
B. policies.
C. strategies.
D. controls.

Answer: C

Explanation:

Prior to setting IT objectives, an enterprise must have established its strategies. Strategies are the high-level plans that define the direction and goals of the enterprise and how it will achieve them. Strategies provide the context and guidance for setting IT objectives, which are the specific and measurable outcomes that IT will deliver to support the strategies. IT objectives should be aligned with and derived from the enterprise strategies, as well as the enterprise vision, mission, and values

Question: 142

An enterprise's board of directors can BEST manage enterprise risk by:

A. mandating board-approved enterprise risk management (ERM) modifications.
B. requiring the establishment of an enterprise risk management (ERM) framework.
C. requiring the establishment of an enterprise-wide program management office.
D. ensuring the cost-effectiveness of the internal control system.

Answer: B

Explanation:

An enterprise's board of directors can best manage enterprise risk by requiring the establishment of an ERM framework. An ERM framework is a methodology that looks at risk management strategically from the perspective of the entire firm or organization. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentialsfor harm that may interfere with an organization's operations and objectives and/or lead to losses. An ERM framework provides structured feedback and guidance to business units, executive management, and board members implementing and managing ERM programs. An ERM framework helps establish a consistent risk management culture, regardless of employee turnover or industry standards. It also often involves making the risk plan of action available to all stakeholders as part of an annual report

Question: 143

A strategic IT-enabled investment is failing due to unforeseen technology problems. What should be the board of directors' FIRST course of action?

A. Terminate the investment.
B. Assess the business risk and options.
C. Approve an investment budget increase.
D. Revise the investment selection process.

Answer: B

Explanation:

The board of directors' first course of action when a strategic IT-enabled investment is failing due to unforeseen technology problems should be to assess the business risk and options. This means that the board should evaluate the impact of the technology problems on the business objectives, benefits, costs, and risks of the investment, as well as the feasibility and desirability of alternative courses of action, such as continuing, modifying, suspending, or terminating the investment. This will help the board to make an informed and rational decision based on the best available information and evidence.

Question: 144

Which of the following MUST be established before implementing an information architecture that restricts access to data based on sensitivity?

A. Risk and control frameworks
B. Probability and impact analysis
C. Classification and ownership
D. Security and privacy policies

Answer: C

Explanation:

Before implementing an information architecture that restricts access to data based on sensitivity, the

enterprise must establish the classification and ownership of the data. Classification is the process of tagging data according to its type, sensitivity, and value to the organization if altered, stolen, or destroyed. It helps the organization understand the risk and impact of data breaches and
comply with relevant regulations. Ownership is the process of assigning roles andresponsibilities for data creation, maintenance, protection, and disposal. It helps the organization ensure accountability and governance of data throughout its lifecycle

Question: 145

A CEO is concerned that IT costs have significantly exceeded budget without resulting benefits. The root causes are an overlap of IT projects and a lack of alignment with business demands. Which of the following would BEST enable remediation of this situation?

A. Require IT business cases be approved by the board of directors.
B. Assign a set of key risk indicators (KRIs) to each new IT project.
C. Conduct a performance assessment of IT projects.
D. Implement an IT portfolio management policy.

Answer: D

Explanation:

Implementing an IT portfolio management policy would best enable remediation of this situation because it would help the organization to establish and adopt a process for measuring and monitoring the value of IT investments. This process would let the organization manage IT investments similarly to a financial portfolio by balancing potential returns, determining if an investment fits the business objectives, and performing a risk assessment. An IT portfolio management policy would also help to avoid overlap and duplication of IT projects by providing a clear and consistent way of prioritizing, categorizing, and aligning them with the enterprise strategy and goals. An IT portfolio management policy would also facilitate the evaluation and reporting of IT performance and benefits realization

Question: 146

Senior management wants to expand offshoring to include IT services as other types of business offshoring have already resulted in significant financial benefits for the enterprise. The CIO is currently midway through a successful five-year strategy that relies heavily on internal IT resources. What should the CIO do NEXT?

A. Reevaluate the offshoring strategy.
B. Abandon the current IT strategy.
C. Continue with the existing IT strategy.
D. Reevaluate the current IT strategy.

Answer: D

Explanation:

The CIO should reevaluate the current IT strategy in light of the senior management's decision to expand offshoring to include IT services. This means that the CIO should assess the impact of offshoring on the existing IT objectives, plans, resources, capabilities, risks, and performance. The CIO should also consider the potential benefits and challenges of offshoring IT services,such as cost reduction, access to talent, quality assurance, communication, coordination, and security. The CIO should then revise the current IT strategy to align with the enterprise's offshoring strategy and goals, and communicate the changes to the relevant stakeholders

Question: 147

Which of the following is the BEST way to ensure the continued usefulness of IT governance reports for stakeholders?

A. Conduct quarterly audits and adjust reporting based on findings.
B. Establish a standard process for providing feedback.
C. Rely on IT leaders to advise when adjustments should be made.
D. Issue frequent service level satisfaction surveys.

Answer: B

Explanation:

The best way to ensure the continued usefulness of IT governance reports for stakeholders is to establish a standard process for providing feedback. This means that the organization should define and communicate the purpose, scope, format, frequency, and distribution of the IT governance reports, and solicit input from the stakeholders on how well the reports meet their information needs and expectations. The feedback process should also include mechanisms for collecting, analyzing, and acting on the feedback, as well as reporting back to the stakeholders on the changes made or planned. This will help to ensure that the IT governance reports are relevant, accurate, timely, and consistent, and that they support the decision-making and accountability of the stakeholders

Question: 148

The use of an IT balanced scorecard enables the realization of business value of IT through:

A. business value and control mechanisms.
B. outcome measures and performance drivers.
C. financial measures and investment management.
D. vision and alignment with corporate programs.

Answer: B

Explanation:

The use of an IT balanced scorecard enables the realization of business value of IT through outcome measures and performance drivers. Outcome measures are the indicators of the results or consequences of the IT activities, such as customer satisfaction, revenue growth, or market share. Performance drivers are the factors that influence or contribute to the outcome measures, such as process efficiency, quality, or innovation. By using an IT balanced scorecard, the organization can link the outcome measures and performance drivers to the IT objectives, strategies, and actions, and monitor and evaluate how well IT delivers value to the business

Question: 149

The CEO of a large enterprise has announced me commencement of a major business expansion that will double the size of the organization. IT will need to support the expected demand expansion.
What should the CIO do FIRST?

A. Review the resource utilization matrix.
B. Recruit IT resources based on the expansion decision.
C. Embed IT personnel in the business units.
D. Update the IT strategic plan to align with the decision.

Answer: D

Explanation:

The CIO should update the IT strategic plan to align with the decision of the CEO to commence a major business expansion that will double the size of the organization. This means that the CIO should review the current IT vision, mission, goals, objectives, strategies, and actions, and assess how they support the business expansion plan. The CIO should also identify the IT opportunities, challenges, risks, and gaps that may arise from the business expansion, and develop appropriate solutions and mitigation measures. The CIO should then revise the IT strategic plan to reflect the changes and ensure that IT is aligned with and contributes to the business growth and success

Question: 150

An enterprise has been focused on establishing an IT risk management framework. Which of the following should be the PRIMARY motivation behind this objective?

A. Promoting responsibility throughout the enterprise for managing IT risk.
B. Increasing the enterprise's risk tolerance level and risk appetite.
C. Engaging executives in examining IT risk when developing policies.
D. Maintaining a complete and accurate risk registry to belief manage IT risk

Answer: A

Explanation:

The primary motivation behind establishing an IT risk management framework is to promote responsibility throughout the enterprise for managing IT risk. An IT risk management framework is a set of principles, processes, and practices that guide and support the identification, analysis, evaluation, treatment, monitoring, and communication of IT-related risks. An IT risk management framework helps to ensure that IT risks are aligned with the enterprise's objectives, strategies, and risk appetite, and that they are effectively managed by the appropriate stakeholders. An IT risk management framework also helps to foster a culture of risk awareness and accountability within the enterprise

Question: 151

Which of the following is MOST important for the effective design of an IT balanced scorecard?

A. On-demand reporting and continuous monitoring
B. Consulting with the CIO
C. Emphasizing the financial results
D. Identifying appropriate key performance indicators (KPIs)

Answer: D

Explanation:

The most important factor for the effective design of an IT balanced scorecard is identifying appropriate key performance indicators (KPIs). KPIs are the measures that reflect the critical success factors of the IT strategy and goals, and that help to monitor and evaluate the IT performance and value. KPIs should be aligned with the four perspectives of the balanced scorecard: financial, customer, internal process, and learning and growth. KPIs should also be SMART: specific,
measurable, achievable, relevant, and time-bound. By choosing the right KPIs, the IT balanced scorecard can provide a comprehensive and balanced view of the IT contribution to the business, and support the decision-making and improvement processes

Question: 152

An IT audit report indicates that a lack of IT employee risk awareness is creating serious security issues in application design and configuration. Which of the following would be the BEST key risk indicator (KRI) to

show progress in IT employee behavior?

A. Number of IT employees attending security training sessions
B. Results of application security testing
C. Number of reported security incidents
D. Results of application security awareness training quizzes

Answer: D

Explanation:

The best key risk indicator (KRI) to show progress in IT employee behavior regarding application security issues is the results of application security awareness training quizzes. This KRI measures the level of knowledge and understanding that IT employees have acquired from the security training sessions, and how well they can apply it to their work. This KRI can also help to identify the gaps and weaknesses in the training content and delivery, and suggest areas for improvement. A high score on the quizzes indicates a high level of IT employee risk awareness and a low likelihood of creating serious security issues in application design and configuration

Question: 153

A strategic systems project was implemented several months ago. Which of the following is the BEST reference for the IT steering committee as they evaluate its level of success?

A. Stakeholder satisfaction surveysB The project's net present value (NPV)
B. The project's business case
C. Operating metrics of the new system

Answer: C

Explanation:

The best reference for the IT steering committee as they evaluate the level of success of a strategic systems project that was implemented several months ago is the project's business case. The business case is the document that outlines the rationale, objectives, benefits, costs, risks, and assumptions of the project. It also defines the expected outcomes and performance indicators that can be used to measure the project's success. By comparing the actual results of the project with the business case, the IT steering committee can determine if the project has met its intended goals, delivered its expected value, and justified its investment

Question: 154

Which of the following is the MOST important reason for selecting IT key risk indicators (KRIs)?

A. Demonstrating the effectiveness of IT risk policies
B. Assessing the current IT controls model
C. Enabling comparison against similar IT KRIs
D. Increasing the probability of achieving IT goals

Answer: D

Explanation:

The most important reason for selecting IT key risk indicators (KRIs) is to increase the probability of achieving IT goals. IT KRIs are metrics that show the level of exposure or likelihood of occurrence of IT-related risks that may affect the achievement of IT objectives. By selecting and monitoring IT KRIs, the organization can identify and

manage the potential threats and opportunities that may impact the IT performance and value. IT KRIs can also help to trigger corrective or preventive actions, communicate risk information, and support decision-making and improvement processes

Question: 155

A large organization with branches across many countries is in the midst of an enterprise resource planning (ERP) transformation. The IT organization receives news that the branches in a country where the impact to the enterprise is to be greatest are being sold. What should be the NEXT step?

A. Update the ERP business case and re-evaluate the ROI.
B. Cancel the ERP transformation and re-allocate project funds.
C. Adjust the ERP implementation plan and budget.
D. Continue with the ERP migration according to plan.

Answer: C

Explanation:

The next step for the IT organization when they receive news that the branches in a country where the impact to the enterprise is to be greatest are being sold is to adjust the ERP implementation plan and budget. This means that the IT organization should assess the implications of the sale on the ERP transformation objectives, scope, timeline, resources, costs, and risks. The IT organization should also communicate with the relevant stakeholders, such as the business units, the vendors, and the buyers, to coordinate and align the ERP activities with the sale process. The IT organization should then revise the ERP implementation plan and budget to reflect the changes and ensure that the ERP transformation delivers value to the remaining enterprise

Question: 156

A marketing enterprise is considering procuring customer information to more accurately target customer communications and increase sales. The data has a very high cost to the enterprise. Which of the following would provide the MOST comprehensive view into the potential value to the organization?

A. Investment services board review
B. Net present value {NPV) calculation
C. Risk assessment results
D. Cost-benefit analysis results

Answer: D

Explanation:

The most comprehensive view into the potential value of procuring customer information for a marketing enterprise would be provided by the cost-benefit analysis results. A cost-benefit analysis is a method of comparing the costs and benefits of a project or decision in monetary terms. It helps to evaluate the feasibility, profitability, and efficiency of the project or decision, and to identify the best alternative among different options. A cost-benefit analysis can also incorporate non-monetary factors, such as social and environmental impacts, by assigning them monetary values or weights. A cost-benefit analysis can show the net benefit (or net cost) of procuring customer information, as well as the benefit-cost ratio, the payback period, and the internal rate of return. These indicators can help the marketing enterprise to assess how well the procurement of customer information aligns with its objectives, strategies, and budget, and how much value it can create for the enterprise and its customers

Question: 157

Which of the following provides the BEST assurance on the effectiveness of IT service management processes?

A. Performance of incident response
B. Continuous monitoring
C. Key risk indicators (KRIs)
D. Compliance with internal controls

Answer: B

Explanation:

Continuous monitoring provides the best assurance on the effectiveness of IT service management processes because it involves collecting, analyzing, and reporting data on the performance, quality, and outcomes of the IT services on an ongoing basis. Continuous monitoring helps to identify and address any issues, gaps, or deviations from the expected standards and goals of the IT service management processes. It also helps to measure and demonstrate the value and impact of the IT services to the customers and stakeholders. Continuous monitoring can also support continuous improvement and innovation of the IT service management processes by providing feedback and insights for decision-making and planning

Question: 158

A rail transport company has the worst on-time arrival record in the industry due to an antiquated IT system that controls scheduling. Despite employee resistance, an initiative lo upgrade the technology and related processes has been approved. To maximize employee engagement throughout the project, which of the following should be in place prior to the start of the initiative? A. Procurement management plan

B. Organizational change management plan
C. Risk response plan
D. Resource management plan

Answer: B

Explanation:

An organizational change management plan is the best option to have in place prior to the start of an initiative to upgrade the technology and related processes of a rail transport company that has
the worst on-time arrival record in the industry due to an antiquated IT system that controls scheduling. An organizational change management plan is a document that outlines the strategy, approach, and actions for managing and implementing a change within an organization. It helps to prepare the organization and its stakeholders for the change, communicate the vision and benefits of the change, address the potential resistance and challenges of the change, and monitorand evaluate the progress and outcomes of the change. An organizational change management plan is especially important for a project that involves a significant technological and process change that may impact the culture, performance, and satisfaction of the employees. By having an organizational change management plan in place before the start of the initiative, the rail transport company can maximize employee engagement throughout the project, and ensure a smooth and successful transition to the new IT system and processes

Question: 159

A financial institution with a highly regarded reputation for protecting customer interests has recently deployed a mobile payments program. Which of the following key risk indicators (KRIs) would be of MOST interest to the CIO?

A. Number of failed software updates on mobile devices
B. Percentage of incomplete transactions
C. Failure rate of point-of-sale systems
D. Total volume of suspicious transactions

Answer: D

Explanation:

The key risk indicator (KRI) that would be of most interest to the CIO of a financial institution with a highly regarded reputation for protecting customer interests that has recently deployed a mobile payments program is the total volume of suspicious transactions. This KRI measures the number and value of transactions that are flagged as potentially fraudulent, malicious, or erroneous by the mobile payments system or by the customers. This KRI reflects the level of security and reliability of the mobile payments program, as well as the customer trust and satisfaction. A high volume of suspicious transactions indicates a high risk of financial losses, reputational damage, regulatory penalties, and customer attrition for the financial institution. Therefore, the CIO should monitor this KRI closely and take appropriate actions to prevent or mitigate any incidents that may compromise the mobile payments program

Question: 160

An enterprise has a large backlog of IT projects. The current strategy is to execute projects as they are submitted, but executive management does not believe this method is optimal. Which of the following is the MOST important action to address this concern?

A. Implement stage-gating to determine the value of each project.
B. Establish a performance dashboard that determines business value.
C. Implement a methodology to prioritize projects based on resource availability.
D. Create a combined business/IT committee to determine project prioritization.

Answer: C

Explanation:

The most important action to address the concern of executive management about the current strategy of executing projects as they are submitted is to create a combined business/IT committee to determine project prioritization. This action will help to ensure that the IT projects are aligned with the enterprise's objectives, strategies, and values, and that they deliver the highest value and impact to the business and the customers. A combined business/IT committee can also facilitate the communication, collaboration, and coordination among the stakeholders involved in the IT projects, and resolve any conflicts or issues that may arise. A combined business/IT committee can use various project prioritization methods, such as scoring models, prioritization matrices, payback periods, or portfolio dashboards, to evaluate and rank the IT projects based on criteria such as business value, urgency, feasibility, risk, and resource availability

Question: 161

An IT strategy committee wants to ensure that a risk program is successfully implemented throughout the enterprise. Which of the following would BEST support this goal?

A. A risk management framework
B. Mandatory risk awareness courses for staff
C. A risk recognition and reporting policy
D. Commitment from senior management

Answer: D

Explanation:

This is because a risk program is a strategic initiative that requires the support and involvement of the top leaders of the enterprise. Senior management can demonstrate their commitment to the risk program by: Providing clear direction and guidance on the objectives, scope, and approach of the risk program Allocating sufficient resources, budget, and authority to the risk program team Communicating the importance and benefits of the risk program to all stakeholders Encouraging a culture of risk awareness and accountability across the enterprise Reviewing and approving the risk program deliverables and outcomes Rewarding and recognizing the achievements and contributions of the risk program team and participants A risk management framework (A) is a tool that helps to define and implement the risk program, but it does not ensure its success without senior management commitment. Mandatory risk awareness courses for staff (B) are a way to increase the knowledge and skills of the staff regarding risk management, but they do not guarantee their engagement and participation in the risk program without senior management endorsement. A risk recognition and reporting policy © is a document that establishes the rules and procedures for identifying and communicatingrisks, but it does not ensure its compliance and effectiveness without senior management oversight.

Question: 162

Which of the following would be the PRIMARY impact on IT governance when a business strategy is changed?

A. Performance outcomes of IT objectives
B. IT governance structure
C. Maturity level of IT processes
D. Relationship level with IT outsourcers

Answer: B

Explanation:

A change in business strategy may require a change in IT governance structure to align with the new direction and objectives of the organization. The other options are not the primary impact of a business strategy change, but rather the outcomes or consequences of IT governance. Reference := ISACA, CGEIT Review Manual, 27th Edition, 2020, page 10.

Question: 163

The MOST successful IT performance metrics are those that:

A. measure financial results.
B. measure all areas.
C. are approved by the stakeholders.
D. contain objective measures.

Answer: D

Explanation:

The most successful IT performance metrics are those that contain objective measures that can be quantified and verified. Objective measures are more reliable, consistent, and repeatable than subjective measures, which may vary depending on the perspective or opinion of the stakeholders. Objective measures also help to align IT performance goals with business goals and to communicate the value of IT to the rest of the organization. According to one source1, a good metric is linear, reliable, repeatable, easy to use, consistent and independent. Reference := ISACA, CGEIT Review Manual, 27th Edition, 2020, page 11; Performance Measurement Metrics for

Question: 164

When implementing an IT governance framework, which of the following would BEST ensure acceptance of the framework?

A. Factoring in the effects of enterprise culture
B. Using subject matter experts
C. Using industry-accepted practices
D. Complying with regulatory requirements

Answer: A

Explanation:

When implementing an IT governance framework, it is important to consider the effects of enterprise culture on the acceptance and adoption of the framework. Enterprise culture is the set of values, beliefs, norms, and behaviors that shape how an organization operates and interacts with its stakeholders. A mismatch between the IT governance framework and the enterprise culture can lead to resistance, conflict, or failure of the framework. Therefore, it is best to factor in the effects of enterprise culture and tailor the framework to suit the specific context and needs of the organization. The other options are not the best way to ensure acceptance of the framework, but rather some of the factors that can influence the design and implementation of the framework. Using subject matter experts, industry-accepted practices, and complying with regulatory requirements can help to ensure
the quality, relevance, and compliance of the framework, but they do not necessarily guarantee its acceptance by the organization. Reference := ISACA, CGEIT Review Manual, 27th Edition, 2020, page 12; Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks

Question: 165

An executive sponsor of a partially completed IT project has learned that the financial assumptions supporting the project have changed. Which of the following governance actions should be taken FIRST?

A. Schedule an interim project review.
B. Request a risk assessment.
C. Re-evaluate the project in the portfolio.
D. Request an update to the business case

Answer: D

Explanation:

The first governance action that should be taken when the financial assumptions supporting a project have changed is to request an update to the business case. The business case is the document that justifies the initiation, continuation, or termination of a project based on its expected costs, benefits, and risks. A change in the financial assumptions may affect the viability and value of the project, and therefore, the business case should be revised to reflect the new situation. The updated business case will then inform the subsequent governance actions, such as scheduling an interim project review, requesting a risk assessment, or re-evaluating the project inthe portfolio. According to one source1, “The business case is a living document and should be reviewed and updated periodically as new information becomes available.” Reference := ISACA, CGEIT Review Manual, 27th Edition, 2020, page 14; Tips for Agile Project Governance

Question: 166

An enterprise has decided to create its first mobile application. The IT director is concerned about the potential impact of this initiative. Which of the following is the MOST important input for managing the risk associated with this initiative?

A. Enterprise architecture (EA)
B. IT risk scorecard
C. Enterprise risk appetite
D. Business requirements

Answer: A

Explanation:

Enterprise architecture (EA) is the most important input for managing the risk associated with creating a mobile application, because it provides a holistic view of the current and future state of the enterprise's IT environment, including its goals, principles, standards, policies, processes, technologies, and systems. EA helps to identify the gaps, dependencies, constraints, and opportunities for the mobile application initiative, and to align it with the enterprise's strategic objectives and business requirements. EA also helps to assess the impact of the mobile application on the existing IT infrastructure, security, performance, and compliance. By using EA as an input for
IT risk management, the enterprise can ensure that the mobile application is designed, developed, deployed, and maintained in a consistent, coherent, and optimal way that minimizes the potential risks and maximizes the expected benefits. The other options are not the most important input for managing the risk associated with creating a mobile application, but rather some of the outputs or outcomes of IT risk management. An IT risk scorecard is a tool that measures and reports the performance of IT risk management activities and controls. An enterprise risk appetite is a statement that defines the level and type of risk that an enterprise is willing to accept or avoid in pursuit of its objectives. Business requirements are the specifications that describe what the mobile application should do and how it should meet the needs and expectations of the users and stakeholders. Reference := ISACA, CGEIT Review Manual, 27th Edition, 2020, page 15; Enterprise Architecture as Business Capabilities Architecture

Question: 167

As the required core competencies of the IT workforce are anticipated and identified, what is the NEXT step in strengthening the department's human resource assets?

A. Develop a responsible, accountable, consulted, and informed (RACI) chart.
B. Create an effective recruitment, retention, and training program.
C. Commit to the board performance metrics and bonus structure.
D. Develop personnel requirements for third-party assurance.

Answer: B

Explanation:

As the required core competencies of the IT workforce are anticipated and identified, the next step in strengthening the department's human resource assets is to create an effective recruitment, retention, and training program. This step involves designing and implementing strategies to attract, develop, and retain employees who have the skills, knowledge, and behaviors that align with the IT department's goals and objectives. A recruitment strategy should focus on sourcing and selecting candidates who have the core competencies needed for the IT roles, as well as the potential to grow and adapt to changing IT needs. A

retention strategy should focus on creating a positive work environment that motivates, engages, and rewards employees for their performance and contributions. A training strategy should focus on providing learning opportunities and resources that enable employees to acquire, enhance, and update their core competencies, as well as to develop new ones that are relevant for the future of IT. The other options are not the next step in strengthening the department's human resource assets, but rather some of the tools or outcomes that can support or result from the recruitment, retention, and training program. A responsible, accountable, consulted, and informed (RACI) chart is a tool that clarifies the roles and responsibilities of different stakeholders in a project or process. A performance metrics and bonus structure is an outcome that measures and rewards the achievement of IT goals and objectives. A personnel requirements for third-party assurance is a tool that defines the qualifications and expectations of external service providers or auditors. Reference := What is Competency Management? Best Practices in 2023 - AIHR1; Digital Talent Framework to Future-Proof the IT Workforce - Gartner

Question: 168

To generate value for the enterprise, it is MOST important that IT investments are:

A. aligned with the IT strategic objectives.
B. approved by the CFO.
C. consistent with the enterprise's business objectives.
D. included in the balanced scorecard.

Answer: C

Explanation:

To generate value for the enterprise, it is most important that IT investments are consistent with the enterprise's business objectives. This means that IT investments should support and enable the achievement of the enterprise's vision, mission, goals, and strategies. IT investments should also align with the enterprise's values, culture, risk appetite, and stakeholder expectations. Byensuring that IT investments are consistent with the enterprise's business objectives, the enterprise can maximize the benefits and value that IT can deliver, and avoid wasting resources on IT projects or initiatives that are not relevant, necessary, or effective. According to one source1, "Driving value creation with technology investments requires a clear understanding of how technology can enable business strategy and create value for the organization." The other options are not the most important factor for generating value for the enterprise, but rather some of the steps or outcomes that can support or result from IT investments. Aligning IT investments with the IT strategic objectives is important, but not sufficient, as the IT strategic objectives should also be aligned with the enterprise's business objectives. Approving IT investments by the CFO is a part of the financial governance process, but it does not guarantee that the IT investments are consistent with the enterprise's business objectives. Including IT investments in the balanced scorecard is a way of measuring and reporting on the performance and value of IT investments, but it does not ensure that the IT investments are consistent with the enterprise's business objectives. Reference := Driving value creation with technology investments

Question: 169

An enterprise plans to implement a business intelligence (BI) tool with data sources from various enterprise applications. Which of the following is the GREATEST challenge to implementation?

A. Interface issues between enterprise and BI applications
B. Large volumes of data fed from enterprise applications
C. The need for staff to be trained on the new BI tool
D. Data definition and mapping sources from applications

Answer: D

Explanation:

Data definition and mapping sources from applications is the greatest challenge to implementing a business intelligence (BI) tool with data sources from various enterprise applications because it involves ensuring the consistency, accuracy, and quality of data across different systems and formats. Data definition and mapping requires defining common data elements, identifying data sources and targets, establishing data transformation rules, and resolving data conflicts and discrepancies. This is a complex and time-consuming process that requires a high level of coordination and collaboration among different stakeholders and data owners.

Reference:

According to ISACA's CGEIT Review Manual 2021, one of the key activities for ensuring effective IT- enabled business innovation is to "define and map data sources from various enterprise applications to the BI tool."1

According to ISACA's COBIT 2019 Framework, one of the governance objectives for managing data is to "ensure that data are defined consistently across the enterprise and that data quality issues are identified and resolved."2

According to ISACA's Business Intelligence: Governance and Analytics guide, one of the challenges for BI governance is to "ensure that data are properly defined, mapped, transformed, integrated, and validated across different sources and systems."3

Question: 170

The use of new technology in an enterprise will require specific expertise and updated system development processes. There is concern that IT is not properly sourced. Which of the following should be the FIRST course of action?

A. Perform a risk assessment on potential outsourcing.
B. Update the enterprise architecture (EA) with the new technology.
C. Review the IT balanced scorecard for sourcing opportunities.
D. Assess the gap between current and required staff competencies.

Answer: D

Explanation:

The first course of action when the use of new technology in an enterprise will require specific expertise and updated system development processes is to assess the gap between current and required staff competencies. This course of action involves identifying the skills, knowledge, and abilities that are needed to implement and manage the new technology, and comparing them with the existing capabilities of the IT staff. By assessing the gap between current and required staff competencies, the enterprise can determine the extent and nature of the sourcing challenge, and plan for appropriate solutions, such as training, hiring, or outsourcing. According to one source1, "A competency gap analysis is a process of identifying the difference between what is required for a person to perform their role effectively and what they actually possess." The other options are not the first course of action when the use of new technology in an enterprise will require specific expertise and updated system development processes, but rather some of the steps or outcomes that can follow or result from the gap assessment. Performing a risk assessment on potential outsourcing is a step that involves evaluating the benefits and drawbacks of delegating some or all of the IT functions related to the new technology to an external service provider. This step can be done after assessing the gap between current and required staff competencies, and identifying outsourcing as a viable option. Updating the enterprise architecture (EA) with the new technology is a step that involves incorporating the new technology into the holistic view of the enterprise's IT environment, including its goals, principles, standards, policies, processes, technologies, and

systems. This step can be done after assessing the gap between current and required staff competencies, and ensuring that the new technology aligns with the enterprise's strategic objectives and business requirements. Reviewing the IT balanced scorecard for sourcing opportunities is an outcome that involves measuring and reporting on the performance and value of IT sourcing activities and outcomes. This outcome can be done after assessing the gapbetween current and required staff competencies, and implementing the chosen sourcing solution. Reference := What is Competency Gap Analysis? Definition & Examples

Question: 171

An enterprise is evaluating a Software as a Service (SaaS) solution to support a core business process. There is no outsourcing governance or vendor management in place. What should be the CEO's FIRST course of action?

A. Ensure the roles and responsibilities to manage service providers are defined.
B. Establish a contract with the SaaS solution provider.
C. Instruct management to use the standard procurement process.
D. Ensure the service level agreements (SLAs) for service providers are defined.

Answer: A

Explanation:

According to the CGEIT certification guide, the CEO's first course of action should be to ensure that there is a clear governance framework for outsourcing and that the roles and responsibilities for managing service providers are defined and assigned. This will help to establish accountability, oversight and control over the SaaS solution and its provider. Reference := CGEIT certification guide, domain 1: Governance of Enterprise IT, section 1.3: Governance Frameworks, page 17.

Question: 172

An IT steering committee wants the enterprise's mobile workforce to use cloud-based file storage to save non-sensitive corporate data, removing the need for remote access to that information. Before this change is implemented, what should be included in the data management policy?

A. A mandate for periodic employee training on how to classify corporate data files
B. A mandate for the encryption of all corporate data files at rest that contain sensitive data
C. A process for blocking access to cloud-based apps if inappropriate content is discovered
D. A requirement to scan approved cloud-based apps for inappropriate content

Answer: D

Explanation:

According to the web search results, a data management policy for cloud-based file storage should include a requirement to scan approved cloud-based apps for inappropriate content. This can help to prevent data leakage, compliance violations, and reputational damage. For example, one of the results1 describes how to use Microsoft Defender for Cloud Apps to create file policies that can monitor and control the data and files in your organization's cloud app use, and apply automated actions for governance and remediation. Another result2 explains how to use Google Cloud Storage's Bucket Lock feature to set a data retention policy for a bucket that governs how long objects in the bucket must be retained, and how to lock the policy to prevent itfrom being reduced or removed. A third result3 outlines the best practices and approval processes for using cloud computing services at Tufts University, and states that "the university reserves the right to scan any cloud computing service used by Tufts faculty, staff, or students for inappropriate content". Reference := File policies - Microsoft Defender for Cloud Apps

Retention policies and retention policy locks | Cloud Storage | Google Cloud Cloud Computing Services Policy | Technology Services - Tufts University

Question: 173

Who is PRIMARILY accountable for delivering the benefits of an IT-enabled investment program to the enterprise?

A. Program manager
B. IT steering committee chair
C. CIO
D. Business sponsor

Answer: D

Explanation:

According to the CGEIT certification guide, the business sponsor is primarily accountable for delivering the benefits of an IT-enabled investment program to the enterprise. The business sponsor is the person who has the authority and responsibility to initiate, influence and approve the business objectives and requirements of the program. The business sponsor also ensures that the program aligns with the enterprise strategy and delivers value to the enterprise1. The program manager, the IT steering committee chair and the CIO are responsible for supporting the business sponsor in delivering the benefits, but they are not primarily accountable for them2. Reference :=
CGEIT certification guide, domain 4: Benefits Realization, section 4.1: Benefits Governance, page 137. CGEIT certification guide, domain 4: Benefits Realization, section 4.2: Benefits Delivery Life Cycle, page 140.

Question: 174

An enterprise incurred penalties for noncompliance with privacy regulations. Which of the following is MOST important to ensure appropriate ownership of access controls to address this deficiency?

A. Authenticating access to information assets based on roles or business rules.
B. Implementing multi-factor authentication controls
C. Granting access to information based on information architecture
D. Engaging an audit of logical access controls and related security policies

Answer: A

Explanation:

According to the web search results, authenticating access to information assets based on roles or business rules is the most important way to ensure appropriate ownership of access controls to address privacy compliance. This is because role-based access control (RBAC) and attribute-based access control (ABAC) are two of the most common and effective methods for enforcing the principle of least privilege, which means granting users only the minimum level of access they need to perform their tasks. This can help to protect the confidentiality, integrity, and availability of information assets, as well as to comply with privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). For example, one of the results1 states that "RBAC is a key component of any organization's compliance strategy, as it helps ensure that only authorized users can access sensitive data and resources". Another result2 explains that "ABAC is a logical model for access control that supports fine-grained authorization based on attributes, environment conditions, and policies". A third result3 discusses how RBAC and ABAC can help organizations achieve privacy compliance by implementing data minimization, purpose limitation, and accountability principles. Reference :=

What Is Access Control? | Microsoft Security
Access Control Policy and Implementation Guides | CSRC
Understanding Data Privacy – A Compliance Strategy Can Mitigate Cyber …

Question: 175

Which of the following would be of MOST concern regarding the effectiveness of risk management processes?

A. Key risk indicators (KRIs) are not established.
B. Risk management requirements are not included in performance reviews.
C. The plans and procedures are not updated on an annual basis.
D. There is no framework to ensure effective reporting of risk events.

Answer: D

Explanation:

According to the web search results, one of the most important aspects of risk management is the timely and accurate reporting of risk events, which are incidents or occurrences that have a negative impact on the objectives, operations, or reputation of an organization1. A framework to ensure effective reporting of risk events can help to identify, analyze, communicate, and respond to risks in a systematic and consistent manner2. Without such a framework, the organization may fail to capture, escalate, and learn from risk events, and may expose itself to greater losses,liabilities, and regulatory sanctions3. Therefore, the lack of a framework to ensure effective reporting of risk events would be of most concern regarding the effectiveness of risk management processes.

The other options are less concerning than option D, although they may also indicate some weaknesses in the risk management processes. Key risk indicators (KRIs) are metrics that measure the likelihood or impact of potential or actual risks4. While they are useful for monitoring and managing risks, they are not essential for the effectiveness of risk management processes. Risk management requirements are criteria or standards that define the expectations and responsibilities for managing risks. Including them in performance reviews can help to align the incentives and behaviors of employees with the risk appetite and strategy of the organization. However, they are not the only way to ensure accountability and compliance with risk management processes. The plans and procedures are documents that describe the objectives, scope, roles, activities, and outputs of risk management processes. Updating them on an annual basis can help to reflect the changes in the internal and external environment that affect the risks faced by the organization. However, they are not the only source of guidance and information for risk management processes. Reference :=

Risk Event - Definition from KWHS
Risk Management - Overview, Importance and Processes Transforming risk efficiency and effectiveness | McKinsey Key Risk Indicators (KRIs) - Definition from KWHS
[Risk Management Requirements - an overview | ScienceDirect Topics] [Risk Management Requirements - an overview | ScienceDirect Topics] [Risk Management Plan - an overview | ScienceDirect Topics] [Risk Management Plan - an overview | ScienceDirect Topics]

Question: 176

An enterprise has a zero-tolerance policy regarding security. This policy is causing a large number of email attachments to be blocked and is a disruption to enterprise. Which of the following should be the FIRST governance step to address this email issue?

A. Direct the development of an email usage policy.
B. Obtain senior management input based on identified risk.
C. Recommend business sign-off on the zero-tolerance policy.
D. Introduce an exception process.

Answer: B

Explanation:

According to the CGEIT certification guide, the first governance step to address the email issue caused by the zero-tolerance policy regarding security is to obtain senior management inputbased on identified risk. This is because senior management is ultimately responsible for setting the risk appetite and tolerance of the enterprise, and for balancing the security and business needs. The zero-tolerance policy may be too restrictive and may not align with the enterprise's risk profile and objectives. Therefore, senior management input is needed to review and adjust the policy according to the risk assessment and analysis1. The other options are less appropriate as the first governance step, as they do not involve senior management input or risk-based decision making. Reference := CGEIT certification guide, domain 3: Risk Optimization, section 3.1: Risk Governance, page 87.

Question: 177

Which of the following is the BEST method for determining an enterprise's current appetite for risk?

A. Interviewing senior management
B. Evaluating the balanced scorecard
C. Reviewing recent audit findings
D. Assessing social media adoption

Answer: A

Explanation:

According to the CGEIT certification guide, the best method for determining an enterprise's current appetite for risk is interviewing senior management. This is because senior management is responsible for setting the risk appetite and tolerance of the enterprise, and for balancing the security and business needs. The risk appetite reflects the amount and type of risk that an organization is willing to take in order to meet their strategic objectives. Interviewing senior management can help to understand their perspectives, expectations, and preferences regarding risk taking1. The other options are less effective than option A, as they do not directly capture the senior management's input or risk-based decision making. Reference := CGEIT certification guide, domain 3: Risk Optimization, section 3.1: Risk Governance, page 87.

Question: 178

Which of the following is the MOST effective approach to ensure senior management sponsorship of IT risk management?

A. Benchmark risk framework against best practices.
B. Calculate financial impact for each IT risk finding.
C. Periodically review the IT risk register entries.
D. Integrate IT risk into enterprise risk management (ERM).

Answer: D

Explanation:

According to the CGEIT certification guide, the most effective approach to ensure senior management sponsorship of IT risk management is to integrate IT risk into enterprise risk management (ERM). This is because ERM is a holistic and strategic approach that considers all types of risks that may affect the achievement of the enterprise's objectives. By integrating IT risk into ERM, senior management can better understand the impact and interdependencies of IT risks on the enterprise's performance and value, and can provide more effective oversight and guidance to the IT risk management processes1. The other options are less effective than option D, as they do not address the alignment and integration of IT risk with the

enterprise's strategy and

objectives. Reference:= CGEIT certification guide, domain 3: Risk Optimization, section 3.1: Risk Governance, page 86.

Question: 179

Which of the following is the MOST effective means for IT management to report to executive management regarding the value of IT?

A. IT process maturity level
B. Cost-benefit analysis
C. Resource assessment
D. Balanced scorecard

Answer: D

Explanation:

According to the CGEIT certification guide, the balanced scorecard is the most effective means for IT management to report to executive management regarding the value of IT. The balanced scorecard is a strategic management tool that translates the vision and strategy of an organization into a comprehensive set of performance measures that provide the framework for a strategic measurement and management system1. The balanced scorecard enables IT management to communicate the value of IT in terms of four perspectives: financial, customer, internal business process, and learning and growth2. The balanced scorecard helps IT management to align IT objectives with business objectives, monitor and improve IT performance, and demonstrate IT contribution to business value3.

The other options are less effective than option D, as they do not provide a comprehensive and balanced view of the value of IT. IT process maturity level is a measure of how well-defined, managed, measured, and optimized an IT process is4. While it can indicate the quality and efficiency of IT processes, it does not directly link them to business outcomes or value. Cost-benefit analysis is a technique that compares the costs and benefits of an IT project or investment. While it can show the financial return of IT initiatives, it does not capture the non-financial aspects of IT value, such as customer satisfaction, innovation, or learning. Resource assessment is a process that evaluates the availability and utilization of IT resources, such as people, technology, or information. While it can show the capacity and capability of IT resources, it does not measure how they support the business strategy or goals.

Reference :=

CGEIT certification guide, domain 4: Benefits Realization, section 4.3: Value Governance, page 147. CGEIT certification guide, domain 4: Benefits Realization, section 4.4: Performance Measurement and Reporting, page 150.

Balanced Scorecard - an overview | ScienceDirect Topics IT Process Maturity - an overview | ScienceDirect Topics [Cost-Benefit Analysis - an overview | ScienceDirect Topics]

[Resource Assessment - an overview | ScienceDirect Topics]

Question: 180

Which of the following is the PRIMARY benefit of communicating the IT strategy across the enterprise?

A. On-time and on-budget delivery of strategic projects
B. Improvement in IT balanced scorecard performance
C. Optimization of IT investment in supporting business objectives
D. Reduced organizational resistance during strategy execution

Answer: D

Explanation:

According to the web search results, the primary benefit of communicating the IT strategy across the enterprise is to reduce organizational resistance during strategy execution. This is because communication can help to create a shared understanding and vision of the IT strategy, and to foster trust and commitment among the stakeholders. Communication can also help to address the concerns and expectations of different groups, and to overcome the barriers and challenges that may arise during the implementation of the IT strategy1. The other options are less important than option D, as they are not directly related to communication, but rather to other factors such as project management, performance measurement, and investment optimization.
Reference := How to Communicate Your Company's Strategy Effectively

Question: 181

The CIO in a large enterprise is seeking assurance that significant IT risk is being proactively monitored and does not exceed agreed risk tolerance levels. The BEST way to provide this ongoing assurance is to require the development of:

A. an IT risk appetite statement.
B. a risk management policy.
C. key risk indicators (KRIs).
D. a risk register.

Answer: C

Explanation:

According to the CGEIT certification guide, key risk indicators (KRIs) are the best way to provide ongoing assurance that significant IT risk is being proactively monitored and does not exceed agreed risk tolerance levels. KRIs are metrics that measure the likelihood or impact of potential or actual risks, and provide early warning signals of increasing risk exposures1. KRIs can help IT management to track and report the status and trends of IT risks, and to trigger timely responses and actions when the risk levels approach or exceed the predefined thresholds2. The other options are less suitable than option C, as they do not provide ongoing assurance or proactive monitoring of IT risk. An IT risk appetite statement is a document that expresses the amount and type of risk that an organization is willing to take in order to meet their strategic objectives3. A risk management policy is a document that defines the principles, framework, and processes for managing risks in an organization. A risk register is a tool that records and tracks the identified risks, their causes, impacts, likelihood, responses, and owners.

Reference :=
CGEIT certification guide, domain 3: Risk Optimization, section 3.4: Risk Monitoring and Assurance, page 98.
Key Risk Indicators (KRIs) - Definition from KWHS
Risk Appetite - an overview | ScienceDirect Topics
Risk Management Policy - an overview | ScienceDirect Topics
Risk Register - an overview | ScienceDirect Topics

Question: 182

The BEST way to ensure an IT steering committee meets enterprise objectives is to:

A. require a member of the committee to have IT governance expertise.
B. benchmark against industry best practices.
C. establish key performance indicators (KPIs).
D. have key business stakeholders represented on the committee.

Answer: D

Explanation:

According to the web search results, the best way to ensure an IT steering committee meets enterprise objectives is to have key business stakeholders represented on the committee. This is because business stakeholders are the ones who define and own the enterprise objectives, and who can provide the strategic direction, guidance, and support for IT initiatives that align with these objectives. Having key business stakeholders represented on the committee can help to ensure that IT decisions are made in the best interest of the enterprise, and that IT projectsdeliver value and benefits to the business12. The other options are less effective than option D, as they do not address the alignment and integration of IT and business objectives. Requiring a member of the committee to have IT governance expertise may be helpful, but not sufficient, to ensure that the committee meets enterprise objectives. IT governance expertise is not a substitute for business knowledge and involvement. Benchmarking against industry best practices may be useful, but not necessary, to ensure that the committee meets enterprise objectives. Industry best practices may not always suit the specific needs and context of the enterprise. Establishing key performance indicators (KPIs) may be important, but not enough, to ensure that the committee meets enterprise objectives. KPIs are metrics that measure the performance and outcomes of IT projects and processes, but they do not guarantee that these projects and processes are aligned with the enterprise objectives.

Reference :=
What is an IT Steering Committee? – BMC Software | Blogs
IT Governance Committee - The Role and Importance of … - Exceeders

Question: 183

Establishing a uniform definition for likelihood and impact through risk management standards PRIMARILY addresses which of the following concerns?

A. Inconsistent categories of vulnerabilities
B. Conflicting interpretations of risk levels
C. Inconsistent data classification
D. Lack of strategic IT alignment

Answer: B

Explanation:

Establishing a uniform definition for likelihood and impact through risk management standards primarily addresses the concern of conflicting interpretations of risk levels. This is because likelihood and impact are two key factors that determine the level of risk associated with a threat or event. Different stakeholders may have different perceptions and expectations of what constitutes a high, medium, or low likelihood or impact, which can lead to inconsistent or inaccurate risk assessment and management. By defining and applying a common set of criteria and scales for likelihood and impact, risk management standards can help to ensure a consistent and objective evaluation and communication of risk levels across the organization

Question: 184

An enterprise embarked on an aggressive strategy requiring the implementation of several large IT projects impacting multiple business processes across all departments. Initially employees were supportive of the strategy, but there is growing fatigue and frustration with the ongoing newcapabilities which must be learned. Which of the following would be the BEST action performed by senior management?

A. Incorporate an organizational change management program.
B. Establish "Reward and Recognition" efforts to boost employee morale.

C. Improve the system development life cycle (SDLC) process.
D. Assess current business and IT competencies.

Answer: A

Explanation:

This is because an organizational change management program is a systematic approach to managing the human side of change and ensuring that the people affected by the change are ready, willing, and able to adopt it1. An organizational change management program can help to address the fatigue and frustration of the employees by providing them with clear communication, stakeholder engagement, training and coaching, leadership support, and feedback mechanisms2. An organizational change management program can also help to increase the success rate and benefits realization of the IT projects by reducing resistance, enhancing collaboration, and improving performance3.

The other options are less effective than option A, as they do not address the root cause of the problem or provide a comprehensive solution. Establishing "Reward and Recognition" efforts to boost employee morale may be helpful, but not sufficient, to overcome the fatigue and frustration of the employees. Rewards and recognition can motivate and appreciate the employees for their efforts and achievements, but they do not necessarily help them to cope with the changes or learn the new capabilities4. Improving the system development life cycle (SDLC) process may be useful, but not relevant, to address the fatigue and frustration of the employees. The SDLC process is a framework that defines the tasks and activities involved in developing, testing, deploying, and maintaining IT systems. While improving the SDLC process can enhance the quality and efficiency of IT systems, it does not directly affect the employees' readiness or willingness to adopt them.

Assessing current business and IT competencies may be important, but not enough, to address the fatigue and frustration of the employees. Assessing competencies can help to identify the gaps and needs of the employees in terms of knowledge, skills, and abilities required for their roles. However, assessing competencies alone does not provide any solutions or support for closing those gaps or meeting those needs.

Question: 185

An enterprise decides to accept the IT risk of a subsidiary located in another country even though it exceeds the enterprise's risk appetite. Which of the following would be the BEST justification for this decision?

A. Risk framework alignment
B. Local market common practices
C. Compliance with local regulations
D. Technical gaps among subsidiaries

Answer: C

Explanation:

The best justification for the enterprise's decision to accept the IT risk of a subsidiary located in another country even though it exceeds the enterprise's risk appetite would be compliance with local regulations. This is because local regulations may impose different or stricter requirements on the subsidiary's IT operations, such as data protection, cybersecurity, or privacy laws. Compliance with local regulations may be mandatory or beneficial for the subsidiary to operate legally and effectively in the foreign market. Therefore, the enterprise may decide to accept the IT risk of the subsidiary as a trade-off for complying with local regulations and avoiding potential penalties or reputational damage12.

The other options are less convincing than option C, as they do not provide a strong rationale for accepting the IT risk of the subsidiary. Risk framework alignment is the process of ensuring that the subsidiary's IT risk management practices are consistent and compatible with the enterprise's IT risk management framework. While this may help to improve the communication and coordination of IT risk management across the

enterprise, it does not justify accepting the IT risk of the subsidiary that exceeds the enterprise's risk appetite. Local market common practices are the norms and standards that prevail in the foreign market where the subsidiary operates. While these may influence the subsidiary's IT risk management decisions, they do not necessarily override the enterprise's risk appetite or strategy. Technical gaps among subsidiaries are the differences or discrepancies in the IT systems, processes, or capabilities of different subsidiaries within the enterprise. While these may pose challenges or risks for the enterprise's IT governance and performance, they do not explain why the enterprise would accept the IT risk of a subsidiary that exceeds its risk appetite.

Question: 186

Which of the following is the MOST valuable input when quantifying the loss associated with a major risk event?

A. Key risk indicators (KRIs)
B. IT environment threat modeling
C. Business impact analysis (BIA) report
D. Recovery time objectives (RTOs)

Answer: C

Explanation:

A business impact analysis (BIA) report is the most valuable input when quantifying the loss associated with a major risk event. A BIA report is a document that identifies and evaluates thepotential effects of disruptions to critical business functions and processes. A BIA report can help estimate the financial, operational, reputational, and legal impacts of a risk event, as well as the recovery time and resources needed to resume normal operations. A BIA report can also help prioritize the recovery strategies and objectives based on the criticality and urgency of the business functions and processes.

The other options are not the most valuable input when quantifying the loss associated with a major risk event. Key risk indicators (KRIs) are metrics that provide an early warning of potential threats to the organization's objectives and performance. KRIs can help monitor and measure the risk exposure and effectiveness of risk management activities, but they do not directly quantify the loss associated with a risk event. IT environment threat modeling is a technique that identifies and analyzes the possible vulnerabilities and attack vectors in an IT system or network. Threat modeling can help improve the security and resilience of IT assets and services, but it does not directly quantify the loss associated with a risk event. Recovery time objectives (RTOs) are the maximum acceptable time frames for restoring business functions and processes after a disruption. RTOs can help determine the recovery priorities and strategies, but they do not directly quantify the loss associated with a risk event.

For more information on BIA and quantifying loss, you can refer to these web sources: What is Business Impact Analysis? Definition, Benefits & Examples Quantifying Loss Associated with Major Risk Event - Exam-Answer Quantifying the Qualitative Technology Risk Assessment - ISACA

Question: 187

To reduce the risk of reputational damage through inappropriate use of social media by employees outside of the workplace, the enterprise approach regarding social media should PRIMARILY focus on;

A. implementing preventative controls.
B. developing policies on social media.
C. implementing a review of processes utilizing social media.
D. ensuring each use of social media is approved by management.

Answer: B

Explanation:

Developing policies on social media is the primary focus of the enterprise approach to reduce the risk of reputational damage by employees outside of the workplace. Policies can define the acceptable and unacceptable use of social media, the roles and responsibilities of employees, and the consequences of policy violations. Policies can also provide guidance and awareness to employees on how to use social media responsibly and ethically. Reference: CGEIT Domain 1: Framework for the Governance of Enterprise IT

Question: 188

An enterprise's internal audit group has scheduled a control review of a payroll system project but has been told to wait until the system is implemented. Which of the following is the GREATEST risk associated with the delay?

A. delay in the development of new key performance indicators (KPIs)
B. Continued dependency on compliant legacy systems
C. Increased cost to mitigate deficiencies
D. Lack of adherence to industry best practices

Answer: C

Explanation:

Delaying the control review of a payroll system project until after its implementation increases the risk of discovering control weaknesses or errors that could have been prevented or corrected earlier. This would result in increased cost to mitigate the deficiencies and ensure the system's reliability and compliance. Reference: CGEIT Domain 4: Risk Optimization

Topic 2, Exam pool B

Question: 189

A board of directors has just received a report indicating that only a small number of IT initiatives have been completed on time and within budget, A third of the projects were cancelled prior to completion, and more than half will cost almost double their original estimates. An analysis has determined that no one is held responsible for the completion of investmentinitiatives, and there is no consistency in execution. Which of the following would BEST help the enterprise address these problems?

A. Establishing a project governance framework
B. Assigning business management to an IT investment review board
C. Establishing an IT risk management plan
D. Aligning IT investment priorities to the business

Answer: A

Explanation:

A project governance framework is a set of principles, policies, roles, responsibilities, and processes that guide, direct, and control the initiation, planning, execution, monitoring, and closure of IT projects. A project governance framework can help the enterprise address the problems of poor project performance, lack of accountability, and inconsistency in execution by:
Providing a clear and consistent structure for managing IT projects across the enterprise
Aligning IT projects with the strategic objectives and priorities of the enterprise

Defining the roles and responsibilities of the project stakeholders, including the board of directors, senior management, project sponsors, project managers, project teams, and end-users
Establishing the criteria and methods for selecting, prioritizing, approving, and funding IT projects Setting the standards and expectations for project planning, execution, quality, risk management, communication, and reporting
Implementing the mechanisms and tools for monitoring, controlling, evaluating, and reviewing IT project performance and outcomes
Ensuring the accountability and transparency of IT project decisions and results

Reference:

According to the CGEIT Review Manual 2022, "Project governance is a subset of IT governance that provides a framework for managing IT projects. Project governance ensures that IT projects are aligned with business objectives; are delivered on time, within budget, and with acceptable quality; and are managed in a consistent and transparent manner."1
According to the ISACA article on Project Governance: An Essential Element of Project Management Success2, "Project governance is an empowering aspect of the project management office (PMO) infrastructure management. It enables effective decision making by providing clarity on roles and responsibilities; it also provides a framework for escalation management."
According to the PMI article on Project Governance: What You Need to Know3, "Project governance is a critical element of any project since it provides a framework for accountabilities and responsibilities associated with an organization's capital investments (projects). It is defined as an integrated framework of processes and tools that address matters essential to successful project delivery."

Question: 190

An enterprise is trying to increase the maturity of its IT process from being ad hoc to being repeatable. Which of the following is the PRIMARY benefit of this change?

A. Process optimization is embedded across the organization.
B. Required outcomes are mapped to business objectives.
C. Process performance is measured in business terms.
D. Required outcomes are more frequently achieved.

Answer: D

Explanation:

Increasing the maturity of IT process from being ad hoc to being repeatable means that the process is documented and followed consistently, resulting in more predictable and reliable outcomes. According to the capability maturity model for the IT governance process, a repeatable level indicates that "required outcomes are more frequently achieved" 1. Reference: CGEIT Domain 1: Framework for the Governance of Enterprise IT

Question: 191

A new chief information officer (CIO) of an enterprise recommends implementing portfolio management after realizing there is no process in place for evaluating investments prior to selection. What should be the PRIMARY strategic goal driving this decision?

A. Maximize value from the combined investments.
B. Standardize processes for investment evaluation.
C. Align investments to the enterprise architecture (EA).
D. Enable transparency within the investment process.

Answer: A

Explanation:

Portfolio management is the process of selecting, prioritizing, monitoring and controlling the projects, programs and other related work that best align with the enterprise's strategic objectives and deliver the most value to the stakeholders. The primary strategic goal of implementing portfolio management is to maximize value from the combined investments by ensuring that they are aligned with the enterprise's vision, mission, goals and values, and that they are optimized in terms of risk, return and resource allocation. Reference: CGEIT Domain 2: IT Resources

Question: 192

Supply chain management has established a supplier policy requiring multiple technology suppliers.
What is the BEST way to ensure the success of this policy?

A. Identity and select suppliers based on cost.
B. Align the vendor selection process with the security policy.
C. Implement a master service agreement.
D. Align enterprise architecture (EA) and procurement strategies.

Answer: D

Explanation:

Aligning EA and procurement strategies is the best way to ensure the success of the supplier policy that requires multiple technology suppliers. EA provides a holistic view of the current and future state of the enterprise's IT architecture, including its business processes, applications, data, infrastructure, and security. Procurement strategies define how the enterprise will acquire the necessary IT resources, services, and solutions from external suppliers. By aligning EA and procurement strategies, the enterprise can ensure that the supplier selection and management are consistent with the enterprise's vision, goals, and requirements, and that the suppliers can deliver value, quality, and innovation to the enterprise. Reference: CGEIT Domain 2: IT Resources

Question: 193

When establishing an enterprise data model, the BEST way to ensure the integrity of data is to:

A. classify information using an agreed-upon schema.
B. implement the highest level of protection to data across the enterprise.
C. establish a privileged access management platform.
D. implement a data loss prevention (DLP) program.

Answer: A

Explanation:

Classifying information using an agreed-upon schema is the best way to ensure the integrity of data when establishing an enterprise data model. A schema is a logical structure that defines how data is organized, stored, and accessed. By using a common schema across the enterprise, data can be standardized, validated, and integrated more easily and consistently. A schema also helps to avoid data duplication, inconsistency, and ambiguity, which can compromise data integrity. Reference: What Is an Enterprise Data Model? [+ Examples] - HubSpot Blog

Question: 194

Which of the following is the BEST indication that enterprise value is being derived from IT?

A. IT strategy supports continuous improvement initiatives
B. Metrics are established for IT performance.
C. Rate of return for projects is achieved.
D. IT services enable business strategy.

Answer: D

Explanation:

Enterprise value is being derived from IT when IT services enable business strategy, meaning that IT supports and enhances the enterprise's vision, mission, goals and objectives. IT services enable business strategy by aligning with the enterprise's needs and expectations, delivering value to the stakeholders and customers, and facilitating innovation and transformation. According to the COBIT 5 framework1, one of the principles of governance of enterprise IT (GEIT) is "meeting stakeholder needs", which implies that enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits, optimization of risk and use of resources1. Therefore, IT services should be designed, delivered and monitored in a way that contributes to the creation of value for the enterprise.

Question: 195

Which of the following should be the FIRST step in planning an IT governance implementation?

A. Assign decision-making responsibilities.
B. Obtain necessary business funding.
C. Define key business performance indicators.
D. Identify business drivers.

Answer: D

Explanation:

Identifying business drivers should be the first step in planning an IT governance implementation, because business drivers are the factors that influence the enterprise's vision, mission, goals and objectives, and determine the direction and scope of its IT strategy. Business drivers can include internal and external factors such as customer needs, market trends, regulatory requirements, competitive pressures, organizational culture, etc. By identifying business drivers, the enterprise can ensure that its IT governance implementation is aligned with its business needs and expectations, and that it delivers value to the stakeholders. According to the COBIT 5 framework1, one of the principles of governance of enterprise IT (GEIT) is "covering the enterprise end-to-end", which implies that GEIT should integrate and align with the enterprise governance system1. Therefore, IT governance implementation should start from understanding the enterprise context and drivers.
Reference: Tips for Implementing IT Governance With COBIT 5 - ISACA

Question: 196

A CIO just received a final audit report that indicates there is inconsistent enforcement of the enterprise's mobile device acceptable use policy throughout all business units. Which of the following should be the FIRST step to address this issue?

A. Incorporate compliance metrics into performance goals.
B. Review the relevance of existing policy.
C. Mandate awareness training for all mobile device users.
D. Implement controls to enforce the policy.

Answer: B

Explanation:

The first step to address the issue of inconsistent enforcement of the enterprise's mobile device acceptable use policy is to review the relevance of the existing policy. A mobile device acceptable use policy is a document that defines the rules and guidelines for using mobile devices, such as smartphones, tablets, and laptops, in the enterprise environment. The policy should cover aspects such as device ownership, security, privacy, compliance, and acceptable and unacceptable
behaviors1. A review of the existing policy can help to identify any gaps, inconsistencies, or ambiguities that may cause confusion or non-compliance among the users. The review can also help to ensure that the policy reflects the current business needs, objectives, and risks of the enterprise, as well as the best practices and standards for mobile device management2. By reviewing the relevance of the existing policy, the enterprise can update and improve the policy to make it more clear, comprehensive, and effective. Reference:
Acceptable Use Policy for Mobile Security for Businesses | Interplay
The essential guide to establishing a mobile device policy - Hexnode Blogs

Question: 197

Which of the following should be the MOST important consideration for a hospital planning to use cloud services and mobile applications?

A. Privacy requirements
B. Data classification
C. Acceptable use policy
D. Internet connectivity

Answer: A

Explanation:

Privacy requirements should be the most important consideration for a hospital planning to use cloud services and mobile applications, because they involve the protection of sensitive and personal health information (PHI) of the patients and staff. PHI is a type of data that is subject to strict regulations and standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US1, the General Data Protection Regulation (GDPR) in the EU2, and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada3. These regulations and standards require the hospital to ensure that PHI is collected, stored, processed, and transmitted in a secure and compliant manner, and that the rights and consent of the data subjects are respected. Using cloud services and mobile applications can pose significant challenges and risks to privacy, such as data breaches, unauthorized access, data loss, data residency, third-party liability, etc. Therefore, the hospital should carefully evaluate the privacy requirements and implications of using cloud services and mobile applications, and adoptappropriate governance, policies, controls, and measures to safeguard PHI in the cloud environment.

Question: 198

An enterprise is developing an ethics program, and the ethical standards have been defined. Which of the following should the enterprise do NEXT?

A. Establish a training and awareness program focused on ethics.
B. Implement an enterprise-wide employee monitoring program.
C. Develop key performance indicators (KPIs) for program implementation.
D. Outline and document consequences for noncompliance.

Answer: A

Explanation:

After defining the ethical standards for an ethics program, the next step for the enterprise should be to establish a training and awareness program focused on ethics. A training and awareness program

can help to communicate the ethical standards to all employees and stakeholders, and educate them on the importance, benefits, and expectations of ethical behavior. A training and awareness program can also help to foster a culture of ethics within the enterprise, and encourage employees to apply the ethical standards in their daily work and decision making. According to ISACA's article on Ethics in IT1, "training is essential to ensure that all staff understand what is expected of them and how to apply ethical principles in their work." Furthermore, according to ISACA's CGEIT Domain 1: Framework for the Governance of Enterprise IT2, "training and awareness are key enablers for embedding an appropriate culture throughout the enterprise." Therefore, establishing a training and awareness program focused on ethics is the best way to implement the ethical standards defined by the enterprise.

Question: 199

Reviewing which of the following should be the FIRST step when evaluating the possibility of outsourcing an IT system?

A. Outsourcing strategy
B. Outsourced business processes
C. Service level agreements (SLAs)
D. IT staff skill sets

Answer: A

Explanation:

Reviewing the outsourcing strategy should be the first step when evaluating the possibility of outsourcing an IT system, because the outsourcing strategy defines the vision, objectives, scope, and approach of outsourcing IT activities and services to external providers. The outsourcing strategy should align with the enterprise's business strategy, IT strategy, and IT governanceframework, and should consider the benefits, risks, costs, and impacts of outsourcing on the enterprise's performance, value, and stakeholders. By reviewing the outsourcing strategy, the enterprise can ensure that outsourcing an IT system is consistent with its strategic direction and goals, and that it can achieve the desired outcomes and benefits from outsourcing. According to ISACA's CGEIT Domain 2: IT Resources1, "the enterprise should have a clear vision of what it wants to achieve from outsourcing and how it will manage the relationship with the service provider." Furthermore, according to ISACA's article on IT Outsourcing2, "the first step in developing an effective IT outsourcing strategy is to understand the business drivers for outsourcing and align them with the enterprise's overall business objectives." Therefore, reviewing the outsourcing strategy is the best way to start evaluating the possibility of outsourcing an IT system. Reference:

IT Outsourcing - ISACA

IT Governance: Definitions, Frameworks and Planning - ProjectManager What is IT governance? A formal way to align IT & business strategy | CIO CGEIT Domain 2: IT Resources

Question: 200

To enable the development of required IT skill sets for the enterprise, it is MOST important to define skill requirements based on:

A. training needs.

B. one set of skills applicable to all IT staff.
C. a best practices framework.
D. each role within the IT department.

Answer: D

Explanation:

To enable the development of required IT skill sets for the enterprise, it is most important to define skill requirements based on each role within the IT department, because different roles may have different responsibilities, tasks, and expectations that require specific skills and competencies. By defining skill requirements based on each role, the enterprise can ensure that the IT staff have the appropriate knowledge, abilities, and experience to perform their roles effectively and efficiently, and to support the enterprise's goals and objectives. According to ISACA's CGEIT Domain 2: IT Resources1, "the enterprise should identify the skills required for each IT role and assess the current and future skill gaps." Furthermore, according to ISACA's article on IT Skills Gap2, "the skills gap is not a one-size-fits-all problem. It varies by industry, organization and department/role." Therefore, defining skill requirements based on each role within the IT department is the best way to enable the development of required IT skill sets for the enterprise. Reference:
IT Skills Gap: Trends, Implications and Best Practices - ISACA
IT Governance: Definitions, Frameworks and Planning - ProjectManager
What is IT governance? A formal way to align IT & business strategy | CIO
CGEIT Domain 2: IT Resources

Question: 201

An enterprise is conducting a SWOT analysis as part of IT strategy development. Which of the following would be MOST helpful to identify opportunities and threats?

A. Risk appetite
B. Internal framework assessment
C. Competitor analysis
D. Critical success factors (CSF)

Answer: C

Explanation:

A SWOT analysis is a technique that analyzes strengths, weaknesses, opportunities, and threats of an organization or a project. Strengths and weaknesses are internal factors that can be controlled or influenced by the organization, while opportunities and threats are external factors that are influenced by the environment, market, or competitors1. Therefore, to identify opportunities and threats, it is most helpful to conduct a competitor analysis, which is a process of researching and evaluating the strengths and weaknesses of the competitors in the same industry or market2. A competitor analysis can help to identify the gaps, trends, and best practices in the market, and to discover potential areas for improvement, innovation, or differentiation2. According to ISACA's CGEIT Domain 1: Framework for the Governance of Enterprise IT3, "the enterprise should analyze its external environment to identify opportunities and threats that may affect its ability to achieve its strategic objectives." Furthermore, according to ISACA's article on IT Strategy, "a competitor analysis can help to understand how the enterprise compares with its peers in terms of IT capabilities, performance, and value." Therefore, a competitor analysis is the best way to identify opportunities and threats as part of IT strategy development.

Question: 202

The CIO of a global technology company is considering introducing a bring your own device (BYOD) program. What should the CIO do FIRST?

A. Ensure the infrastructure can meet BYOD requirements.
B. Establish a business case.
C. Define a clear and inclusive BYOD policy.
D. Focus on securing data and access to data.

Answer: B

Explanation:

The CIO should first establish a business case for the BYOD program, because a business case is a document that outlines the rationale, objectives, benefits, costs, risks, and feasibility of a proposed project or initiative1. A business case can help the CIO to justify the need and value of the BYOD program to the senior management and stakeholders, and to secure the necessary funding and resources for its implementation. A business case can also help the CIO to define the scope, requirements, and success criteria of the BYOD program, and to align it with the enterprise's strategy, goals, and governance framework2. According to ISACA's CGEIT Domain 2: IT Resources3, "the enterprise should have a clear business case for each IT investment decision that includes expected benefits, costs, risks and alignment with strategic objectives." Furthermore, according to ISACA's article on BYOD, "a business case is essential for any BYOD initiative as it helps to determine whether the benefits outweigh the costs and risks." Therefore, establishing a business case is the best first step for the CIO who is considering introducing a BYOD program.

Question: 203

What is the BEST way for an IT governance board to establish standards of behavior for the adoption of artificial intelligence (AI)?

A. Direct the creation and approval of an ethical use policy.
B. Review and update the data privacy policy to align with industry standards.
C. Include specific ethics clauses in vendor agreements and contracts.
D. Include ethics topics within onboarding and awareness training.

Answer: A

Explanation:

The best way for an IT governance board to establish standards of behavior for the adoption of artificial intelligence (AI) is to direct the creation and approval of an ethical use policy. An ethical use policy is a document that defines the principles, values, and guidelines for the responsible and ethical design, development, and deployment of AI systems and applications within the enterprise. An ethical use policy can help to ensure that AI is aligned with the enterprise's mission, vision, goals, and values, and that it respects the rights, dignity, and interests of all stakeholders, including customers, employees, partners, regulators, and society at large. An ethical use policy can also help to address the potential risks, challenges, and impacts of AI on various aspects such as privacy, security, fairness, accountability, transparency, trustworthiness, human dignity, human agency, social good, etc. According to ISACA's article on Developing an Artificial Intelligence Governance Framework1, "an ethical use policy is essential for any enterprise that wants to adopt AI in a responsible and sustainable manner. An ethical use policy can help to establish trust and confidence in AI among the stakeholders and customers, and to avoid or mitigate any negative consequences or harms that may arise from AI." Furthermore, according to ISACA's article on Governance of Responsible AI: From EthicalGuidelines to Legal Frameworks2, "an ethical use policy can provide a common framework and language

for the governance of AI across different domains, sectors, and regions. An ethical use policy can also facilitate the compliance with existing laws and regulations that may apply to AI." Therefore, directing the creation and approval of an ethical use policy is the best way for an IT governance board to establish standards of behavior for the adoption of AI.

Question: 204

An IT steering committee is preparing to review proposals for projects that implement emerging technologies. In anticipation of the review, the committee should FIRST:

A. determine if the IT staff can support the emerging technologies.
B. understand how the emerging technologies will influence risk across the enterprise.
C. require a capacity plan and framework review for the emerging technologies,
D. require a review of the enterprise risk management framework.

Answer: B

Explanation:

The first step for the IT steering committee to review proposals for projects that implement emerging technologies is to understand how the emerging technologies will influence risk across the enterprise. Emerging technologies are new or evolving technologies that have the potential to create significant value or disruption for the enterprise, such as artificial intelligence, blockchain, cloud computing, etc. Emerging technologies can also introduce new or increased risks, such as security, privacy, compliance, ethical, operational, strategic, etc. Therefore, the IT steering committee should understand the nature, scope, and impact of these risks, and how they affect the enterprise's risk appetite, tolerance, and profile. By understanding the risk implications of emerging technologies, the IT steering committee can evaluate the proposals more effectively and objectively, and ensure that they align with the enterprise's strategy, goals, and governance framework. According to ISACA's CGEIT Domain 4: Risk Optimization1, "the enterprise should identify and assess the risks associated with emerging technologies and their potential impact on the enterprise's objectives and performance." Furthermore, according to ISACA's article on Emerging Tech Risk2, "the IT steering committee should have a clear understanding of the risk landscape of emerging technologies and how they affect the enterprise's risk posture and appetite." Therefore, understanding how the emerging technologies will influence risk across the enterprise is the best first step for the IT steering committee to review proposals for projects that implement emerging technologies. Reference: Emerging Tech Risk - ISACA

IT Governance: Definitions, Frameworks and Planning - ProjectManager What is IT governance? A formal way to align IT & business strategy | CIO CGEIT Domain 4: Risk Optimization

Question: 205

Which of the following provides the MOST comprehensive insight into the effectiveness of IT?

A. IT balanced scorecard
B. IT strategy
C. Return on investment (ROI)
D. Key risk indicators (KRIs)

Answer: A

Explanation:

An IT balanced scorecard (BSC) is a framework that measures and manages the performance and value of IT in relation to the enterprise's strategy, goals, and objectives. An IT BSC provides the most comprehensive insight into the effectiveness of IT, because it covers four perspectives that reflect the key aspects of IT: financial, customer, internal process, and learning and growth. For each perspective, an IT BSC defines objectives,

measures, targets, and initiatives that align with the enterprise's vision and mission. An IT BSC also helps to balance the short-term and long-term outcomes of IT, as well as the leading and lagging indicators of IT performance. According to ISACA's article on The IT Balanced Scorecard1, "the IT BSC is a powerful tool for demonstrating the contribution of IT to the business, communicating IT performance in business terms, and aligning IT with business strategy." Furthermore, according to ISACA's CGEIT Domain 1: Framework for the Governance of Enterprise IT2, "the IT BSC is a widely used framework for measuring and managing the performance of IT resources in relation to enterprise goals." Therefore, an IT BSC is the best way to provide a comprehensive insight into the effectiveness of IT.

Question: 206

Establishing a uniform definition for likelihood and impact BEST enables an enterprise to:

A. reduce variance in the assessment of risk.
B. develop key risk indicators (KRIs).
C. prioritize threat assessment.
D. reduce risk appetite and tolerance levels.

Answer: A

Explanation:

Establishing a uniform definition for likelihood and impact best enables an enterprise to reduce variance in the assessment of risk. This means that the enterprise can have a consistent and comparable way of measuring and evaluating the probability and consequence of potential events that may affect its objectives, operations, and performance. A uniform definition of likelihood and impact can help to avoid confusion, ambiguity, or bias in the risk assessment process, as well as to improve the quality and reliability of the risk data and analysis.

Some references for establishing a uniform definition for likelihood and impact are:
Risk Assessment: Likelihood & Impact, which provides a guide on how to conduct a risk assessment using a clear formula that involves likelihood and impact1.
Risk = Likelihood x Impact, which explains how to calculate the total amount of risk exposure using likelihood and impact2.
How Analysis, Likelihood, and Impact Models Work Together, which describes how to use different models to express the chance, consequence, and score of a risk3.

Question: 207

An enterprise-wide strategic plan has been approved by the board of directors. Which of the following would BEST support the planning of IT investments required for the enterprise?

A. Service-oriented architecture
B. Enterprise architecture (EA)
C. Contingency planning
D. Enterprise balanced scorecard

Answer: B

Explanation:

Enterprise architecture (EA) is the best option to support the planning of IT investments required for the enterprise, because EA is a practice and a discipline that describes and documents the current and future state of the enterprise's business processes, applications, data, infrastructure, and security, and how they align with the enterprise's vision, mission, goals, and objectives. EA can help the enterprise to plan IT investments by

providing a holistic view of the enterprise's IT architecture, identifying the gaps, needs, and opportunities for improvement, innovation, or transformation, and prioritizing and selecting the IT projects, programs, and portfolios that deliver the most value to the stakeholders and customers. According to ISACA's CGEIT Domain 2: IT Resources1, "EA is a key enabler for IT investment planning and decision making. EA helps to ensure that IT investments are aligned with business strategy and support business outcomes." Furthermore, according to ISACA's article on EA2, "EA can help to optimize IT spending by reducing complexity, duplication, and waste, and by increasing efficiency, agility, and interoperability." Therefore, EA is the best way to support the planning of IT investments required for the enterprise.

Question: 208

An enterprise is concerned with the potential for data leakage as a result of increased use of social media in the workplace, and wishes to establish a social media strategy. Which of the following should be the MOST important consideration in developing this strategy?

A. Criticality of the information
B. Ensuring that the enterprise architecture (EA) is updated
C. Data ownership
D. The balance between business benefits and risk

Answer: D

Explanation:

This is because social media can offer many advantages for an enterprise, such as enhancing customer engagement, increasing brand awareness, improving market intelligence, and fostering innovation. However, social media also poses many challenges and threats, such as data breaches, privacy violations, reputational damage, legal liabilities, and compliance issues. Therefore, an enterprise needs to balance the business benefits and risk of using social media in the workplace, and establish a clear and consistent social media policy and governance framework that defines the objectives, roles, responsibilities, standards, and processes for managing social media activities and data.

Some of the sources that support this answer are:

1: This source provides a comprehensive guide on how to create a social media governance plan that covers the key elements of a social media policy, compliance management, security and risk mitigation, decision-making and approval workflow, and crisis management.

2: This source discusses the gaps, risks, and opportunities of social media governance in the context of Australian public communication. It identifies some of the best practices and recommendations for developing and implementing a social media strategy that aligns with the organizational goals and values, as well as the legal and ethical obligations.

3: This source explores the social media governance challenges and solutions for financial services companies. It highlights the importance of balancing the business benefits and risk of social media, and suggests some of the key steps to achieve effective social media governance, such as conducting a risk assessment, defining a social media policy, establishing a governance structure, monitoring and measuring performance, and reviewing and updating the strategy.

Question: 209

The CIO of an international enterprise is considering the use of an offshore cloud service provider to store customer data. Which of the following should be the MOST important consideration when making this decision?

A. IT service delivery roles and responsibilities
B. Compliance with applicable legislation

C. Likelihood of natural disasters
D. The cloud service provider's reputation

Answer: B

Explanation:

Storing customer data in an offshore cloud service provider may pose legal and regulatory risks for the enterprise, such as data protection, privacy, and sovereignty issues. The CIO should consider the compliance requirements of the applicable legislation in both the home and host countries before making this decision.

Reference :=

CGEIT Review Manual (Digital Version), Chapter 5: Risk Optimization, Section 5.2: IT Risk Management, Subsection 5.2.3: IT Risk Identification, Page 163

CGEIT Review Manual (Print Version), Chapter 5: Risk Optimization, Section 5.2: IT Risk Management, Subsection 5.2.3: IT Risk Identification, Page 163

Question: 210

Which of the following BEST indicates the success of an enterprise's IT governance framework after implementation?

A. A high percentage of business owners involved with the approval of the IT strategic plan
B. A high percentage of IT systems complying with corporate information security standards
C. A high percentage of IT projects delivered on time and on budget
D. A high percentage of IT investments delivering expected benefits

Answer: D

Explanation:

The success of an enterprise's IT governance framework is ultimately measured by the extent to which it enables the achievement of enterprise goals and objectives. One of the key aspects of IT governance is ensuring that IT investments are aligned with business needs and deliver value to the enterprise. Therefore, a high percentage of IT investments delivering expected benefits indicates that the IT governance framework is effective and successful. Reference :=

CGEIT Review Manual (Digital Version), Chapter 1: Framework for the Governance of Enterprise IT, Section 1.1: Introduction to GEIT, Subsection 1.1.2: Benefits of GEIT, Page 9

CGEIT Review Manual (Print Version), Chapter 1: Framework for the Governance of Enterprise IT, Section 1.1: Introduction to GEIT, Subsection 1.1.2: Benefits of GEIT, Page 9

Developing an effective IT governance framework - Wavestone1

Question: 211

Which of the following aspects of IT governance BEST addresses the potential intellectual property implications of a cloud service provider having a database in another country?

A. Contract management
B. Continuity planning
C. Data management
D. Security architecture

Answer: C

Explanation:

Data management is the aspect of IT governance that BEST addresses the potential intellectual property implications of a cloud service provider having a database in another country. Data management involves defining and implementing policies and processes for the effective and efficient acquisition, storage, distribution, usage, and disposal of data in alignment with business objectives and regulatory requirements1. Data management also includes ensuring the protection of data quality, integrity, availability, confidentiality, and ownership1. Therefore, data management can help mitigate the risks of intellectual property infringement, theft, or misuse that may arise from storing data in a foreign jurisdiction with different legal and regulatory frameworks23. Reference := CGEIT Review Manual (Digital Version), Chapter 4: Value Optimization, Section 4.2: IT Value Delivery, Subsection 4.2.3: IT Resource Management, Page 123
CGEIT Review Manual (Print Version), Chapter 4: Value Optimization, Section 4.2: IT Value Delivery, Subsection 4.2.3: IT Resource Management, Page 123
Cloud computing: A brief overview of intellectual property issues "in the cloud" - Lexology2 Protecting Intellectual Property in the Cloud - WIPO

Question: 212

After shifting from lease to purchase of IT infrastructure and software licenses, an enterprise has to pay for unexpected lease extensions causing significant cost overruns. The BEST direction for the IT steering committee would be to establish;

A. an end-of-life program to remove aging infrastructure from the environment.
B. budget cuts to compensate for the cost overruns.
C. a program to annually review financial policy on overruns.
D. a policy to consider total cost of ownership (TCO) in investment decisions.

Answer: D

Explanation:

Total cost of ownership (TCO) is the purchase price of an asset plus the costs of operation over its lifespan1. TCO includes hardware and software acquisition, management and support, communications, end-user expenses and the opportunity cost of downtime, training and other productivity losses2. By considering TCO in investment decisions, an enterprise can avoid unexpected costs and optimize the value of its IT assets3. A policy to consider TCO in investment decisions can
help the enterprise to plan ahead for the lease or purchase of ITinfrastructure and software licenses, and avoid cost overruns due to lease extensions or other factors. Reference :=
CGEIT Review Manual (Digital Version), Chapter 4: Value Optimization, Section 4.2: IT Value Delivery, Subsection 4.2.3: IT Resource Management, Page 123
CGEIT Review Manual (Print Version), Chapter 4: Value Optimization, Section 4.2: IT Value Delivery, Subsection 4.2.3: IT Resource Management, Page 123
How to Calculate Total Cost of Ownership for Software - GetApp4
Total Cost of Ownership: How It's Calculated With Example - Investopedia1

Question: 213

Which of the following is MOST important to the successful implementation of enterprise architecture (EA)?

A. Developing data modeling tools
B. Managing the challenge of change
C. Reducing the cost of IT investments
D. Establishing key performance indicators (KPIs)

Answer: B

Explanation:

Enterprise architecture (EA) is the process of aligning business and IT strategies, processes, and resources to achieve organizational goals and objectives1. EA implementation involves a significant amount of change in the enterprise, such as introducing new technologies, standards, policies, roles, and responsibilities2. Therefore, managing the challenge of change is MOST important to the successful implementation of EA, as it requires effective communication, stakeholder engagement, change management, and governance mechanisms34. Without managing the challenge of change, EA implementation may face resistance, confusion, conflict, or failure. Reference :=

Entreprise Architecture: Critical Factors and Implementation | IEEE …5

A Review of Critical Success Factors of Enterprise Architecture …3

Critical Success Factors of Enterprise Architecture Implementation - IJOCIT1

EVALUATION OF ENTERPRISE ARCHITECTURE IMPLEMENTATION: A CRITICAL …4

Question: 214

The BEST time to identity metrics to measure the performance of an IT-enabled investment is during:

A. system implementation
B. project initiation
C. investment feasibility analysis
D. business case development.

Answer: D

Explanation:

The BEST time to identify metrics to measure the performance of an IT-enabled investment is during business case development. A business case is a document that provides the rationale and justification for initiating a project or investment1. It includes information such as the objectives, scope, benefits, costs, risks, assumptions, and success criteria of the proposed project or investment2. Identifying metrics to measure the performance of an IT-enabled investment during
business case development can help to:

Define the expected outcomes and value of the investment3

Establish a baseline and targets for comparison and evaluation4

Align the investment with the strategic goals and objectives of the enterprise5

Communicate and demonstrate the benefits and impacts of the investment to stakeholders

Monitor and control the progress and performance of the investment throughout its lifecycle Reference :=

Business Case Development - Project Management Institute1

How to Write a Business Case - ProjectManager.com2

How to Measure the Value of an IT Investment - TechSoup3

Maximizing IT Performance: 11 Metrics and KPIs to Monitor - Whatfix4

Top 10 Essential IT Metrics & KPIs - Apptio5

17 Metrics For Evaluating The Success Of Tech Projects And … - Forbes

8 Portfolio Performance Metrics Investors Should Understand - Navexa

Question: 215

To meet the growing demands of a newly established business unit, IT senior management has been tasked with changing the current IT organization model to
service-oriented. With significant growth expected of the IT organization, which of the following is the MOST

Watermark Sample

important consideration when planning for long-term IT service delivery?

A. The IT service delivery model is approved by the business.
B. An IT risk management process is in place.
C. IT is able to provide a comprehensive service catalog to the business.
D. The IT organization is able to sustain business requirements.

Answer: D

Explanation:

The MOST important consideration when planning for long-term IT service delivery is the ability of the IT organization to sustain business requirements. A service-oriented IT organization model is one that focuses on delivering value and outcomes to the business through IT services that are aligned with business needs and expectations1. To achieve this, the IT organization must be able to adapt to the changing and growing demands of the business, as well as the advances in technology and innovation. The IT organization must also have the necessary resources, capabilities, processes, and governance mechanisms to ensure the quality, reliability, availability, security, and performance of the IT services2. Therefore, the ability of the IT organization to sustain business requirements is essential for long-term IT service delivery.

The other options are not as important as option D. While it is important to have the approval of the business, an IT risk management process, and a comprehensive service catalog, these are not sufficient to ensure long-term IT service delivery. They are rather means to achieve the end goal of satisfying and sustaining business requirements. Reference := Make the IT function service-oriented - @CIOPortfolio1 What is SOA (Service-Oriented Architecture)? | IBM

Question: 216

When preparing a new IT strategic plan for board approval, the MOST important consideration is to ensure the plan identifies:

A. roles and responsibilities that link to IT objectives.
B. specific resourcing requirements for identified IT projects.
C. frameworks that will be aligned to IT programs.
D. implications of the strategy on the procurement process.

Answer: A

Explanation:

When preparing a new IT strategic plan for board approval, the MOST important consideration is to ensure the plan identifies roles and responsibilities that link to IT objectives. A well-defined IT strategic plan should clearly articulate the vision, mission, goals, and objectives of the IT function, as well as the strategies and actions to achieve them1. However, without assigning roles and responsibilities to the relevant stakeholders, the plan may lack accountability, ownership, and alignment2. Therefore, it is crucial to identify who is responsible for what, how they will collaborate and communicate, and how they will be measured and rewarded3. This can help to ensure the successful execution and monitoring of the IT strategic plan, as well as the alignment with the business strategy and expectations4.

The other options are not as important as option A. While it is useful to have specific resourcing requirements, frameworks, and implications of the strategy on the procurement process, these are more operational and tactical aspects that can be determined later in the implementation phase.They are not essential for the board approval of the IT strategic plan, which should focus more on the strategic direction and value proposition of the IT function. Reference := How to Write an Information Technology (IT) Business Proposal | Examples1 The Role of Board Approval in the Strategic Planning Process - Veralon2 How To Get The Board To Say Yes - Gartner3

The Board's Role in Strategy | WATSON4
Overseeing strategy: A framework for boards of directors - CPA Canada

Question: 217

Which of the following should be done FIRST when defining responsibilities for ownership of information and systems?

A. Require an information risk assessment.
B. Identify systems that are outsourced.
C. Ensure information is classified.
D. Require an inventory of information assets.

Answer: D

Explanation:

The FIRST step when defining responsibilities for ownership of information and systems is to require an inventory of information assets. An information asset is any data, device, or other component of the environment that supports information-related activities1. An inventory of information assets is a comprehensive list of all the information assets that an organization owns, controls, or uses2. By creating an inventory of information assets, an organization can:
Identify the types, locations, formats, and volumes of information assets3
Determine the value, sensitivity, and criticality of information assets4
Assign ownership and accountability for information assets5
Establish appropriate security controls and protection measures for information assets6
Monitor and audit the usage and lifecycle of information assets7
The other options are not as important as option D. While it is important to require an information risk assessment, identify systems that are outsourced, and ensure information is classified, these are subsequent steps that depend on the availability and accuracy of the inventory of information assets. Without an inventory of information assets, it would be difficult to perform a risk assessment, identify outsourced systems, or classify information according to its value and sensitivity. Reference :=
Information Asset - an overview | ScienceDirect Topics1
Information Asset Inventory - NIST CSRC2
How to Create an Information Asset Inventory - Infosec Resources3
Information Asset Valuation: A Methodology - ISACA4
Data Ownership: Considerations for Risk Management - ISACA5
Information Asset Protection - NIST CSRC6
Information Asset Management - NIST CSRC7

Question: 218

An enterprise is about to complete a major acquisition, and a decision has been made that both companies will be using the parent company's IT infrastructure. Which of the following should be done NEXT?

A. Update the enterprise architecture (EA).
B. Perform a business impact analysis (BIA.
C. Conduct a gap analysis.
D. Develop a communication plan to support the merger.

Answer: C

Explanation:

A gap analysis is the process of comparing the current state and the desired state of an organization or a system, and identifying the gaps or differences between them1. A gap analysis can help to determine the actions and resources needed to bridge the gaps and achieve the desired outcomes2. In the context of an IT infrastructure integration after a major acquisition, a gap analysis can help to: Assess the compatibility and interoperability of the IT systems, applications, data, and processes of both companies3 Identify the gaps, risks, issues, and opportunities related to the IT infrastructure integration4 Prioritize and plan the IT infrastructure integration activities and projects5 Align the IT infrastructure integration with the business goals and objectives of the acquisition Therefore, conducting a gap analysis should be done NEXT after deciding that both companies will be using the parent company's IT infrastructure.

The other options are not as important as option C. While it is important to update the enterprise architecture (EA), perform a business impact analysis (BIA), and develop a communication plan to support the merger, these are subsequent steps that can be done after conducting a gap analysis. A gap analysis can provide valuable inputs and insights for these steps, such as the current and target EA, the potential impacts of the IT infrastructure integration on the business operations and stakeholders, and the communication needs and channels for the IT infrastructure integration. Reference :=

What is Gap Analysis? Definition, Methodology & Examples | ASQ1

Gap Analysis: How to Bridge the Gap Between Performance and …2 How to Make a Successful IT Integration Strategy for Mergers and …4 M&A: The Six Phases of IT Integration - Interlink Cloud Blog3 Post-Merger Integration: M&A Integration Process Guide - DealRoom5 Success Factors for Integrating IT Systems After a Merger | CIO

Question: 219

Following a strategic planning session, new IT objectives were announced. Which of the following is the MOST effective way for the CIO to ensure these objectives are cascaded to IT personnel?

A. Communicate the new IT objectives during a staff meeting.
B. Define individual performance measures related to the IT objectives.
C. Establish IT management's performance measures based on the IT objectives.
D. Update the IT balanced scorecard to align with the new IT objectives.

Answer: B

Explanation:

The MOST effective way for the CIO to ensure that the new IT objectives are cascaded to IT personnel is to define individual performance measures related to the IT objectives. Cascading goals is a framework to get everyone in an organization aligned with the big picture organizational goal, and to make sure they know what to do by breaking strategy into clear tasks and deliverables1. By defining individual performance measures related to the IT objectives, the CIO can: Communicate the expectations and priorities of the IT function to each IT staff member2 Link the individual goals and activities to the IT objectives and the organizational strategy3 Motivate and empower the IT staff to take ownership and responsibility for their work4 Monitor and evaluate the progress and performance of the IT staff and provide feedback and recognition5

The other options are not as effective as option B. While it is important to communicate the new IT objectives, establish IT management's performance measures, and update the IT balanced scorecard, these are not sufficient to ensure that the IT objectives are cascaded to IT personnel. They are rather means to achieve the end goal of aligning and measuring the IT objectives at different levels of the organization. They do not necessarily translate into clear and specific actions and outcomes for each individual IT staff member.

Question: 220

When deciding to develop a system with sensitive data, which of the following is MOST important to include in a business case?

A. A risk assessment to determine the appropriate controls
B. Updated enterprise architecture (EA)
C. Skills gap analysis
D. The additional cost of encrypting sensitive data

Answer: A

Explanation:

When deciding to develop a system with sensitive data, the MOST important thing to include in a business case is a risk assessment to determine the appropriate controls. A business case is a document that provides the rationale and justification for initiating a project or investment1. It includes information such as the objectives, scope, benefits, costs, risks, assumptions, and success criteria of the proposed project or investment2. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and impacts that could affect the project or investment3. A risk assessment can help to:

Identify the sources and types of risks associated with developing a system with sensitive data, such as data breaches, data loss, data corruption, unauthorized access, compliance violations, etc.4 Analyze the likelihood and severity of the risks occurring and their consequences on the project or investment5

Evaluate the current and planned controls to mitigate or prevent the risks, such as encryption, access control, data backup, data activity monitoring, etc.

Prioritize the risks and controls based on their importance and urgency

Communicate and document the risks and controls to stakeholders and decision-makers Therefore, a risk assessment to determine the appropriate controls is essential for developing a business case for a system with sensitive data, as it can help to demonstrate the feasibility, viability, and desirability of the project or investment.

The other options are not as important as option A. While it is useful to have an updated enterprise architecture (EA), a skills gap analysis, and the additional cost of encrypting sensitive data, these are more operational and tactical aspects that can be determined later in the implementation phase. They are not critical for developing a business case for a system with sensitive data, which should focus more on the strategic direction and value proposition of the project or investment. Reference := How to Write a Business Case - ProjectManager.com2 Business Case Development - Project Management Institute1 What is Risk Assessment? Definition & Examples | ASQ3

Data Security: How to Secure Sensitive Data - DATAVERSITY4

Risk Analysis: Definition & Examples | ASQ5

Data access control and data activity monitoring - IBM Cloud …

Risk Evaluation: Definition & Examples | ASQ

Risk Communication: Definition & Examples | ASQ

Question: 221

Which of the following provides the BEST evidence of an IT risk-aware culture across an enterprise?

A. Business staff report identified IT risks.
B. IT risks are communicated to the business.
C. IT risk-related policies are published.
D. The IT infrastructure is resilient.

Answer: A

Explanation:

An IT risk-aware culture is one that promotes a shared understanding of risk and supports the organization's strategy, business model, operational practices, and competitive advantage1. It works to strengthen the core of an organization's operations and protects customers, the brand, and the bottom line1. An IT risk-aware culture also involves the participation and collaboration of all stakeholders in identifying, assessing, and managing IT risks2. Therefore, the BEST evidence of an IT risk-aware culture across an enterprise is when business staff report identified IT risks. This indicates that the business staff are aware of the potential threats and impacts that IT risks can pose to the organization, and that they are willing and able to communicate and escalate them to the appropriate authorities3.

The other options are not as good as option A. While it is important to communicate IT risks to the business, publish IT risk-related policies, and ensure the resilience of the IT infrastructure, these are not sufficient to demonstrate an IT risk-aware culture across an enterprise. They are rather means to achieve the end goal of managing and mitigating IT risks. They do not necessarily reflect the level of awareness, attitude, and behavior of the organization's employees toward risk and how risk is managed within the organization.

Reference := Cultivating a Risk Intelligent Culture - Deloitte US1 Building an Effective Risk-Aware Culture - Magazine4

7 Steps to Create a Risk-Aware Culture | Treasury & Risk3

Question: 222

An IT strategy committee wants to evaluate how well the IT department supports the business strategy. Which of the following is the BEST method for making this determination?

A. Capability maturity assessment
B. Customer survey analysis
C. IT balanced scorecard reporting
D. IT controls assurance program

Answer: C

Explanation:

The BEST method for the IT strategy committee to evaluate how well the IT department supports the business strategy is to use IT balanced scorecard reporting. An IT balanced scorecard (BSC) is a strategic management tool that translates the IT vision and mission intomeasurable objectives, indicators, targets, and initiatives across four perspectives: financial, customer, internal process, and learning and growth1. An IT balanced scorecard reporting is a process of collecting, analyzing, and communicating the performance data and results of the IT department based on the IT BSC framework2. An IT balanced scorecard reporting can help to:

Align the IT objectives and activities with the business strategy and expectations3 Monitor and evaluate the efficiency, effectiveness, and value of the IT department Identify the strengths, weaknesses, opportunities, and threats of the IT department Communicate and demonstrate the contribution and impact of the IT department to the business outcomes

Therefore, an IT balanced scorecard reporting is the most suitable method for the IT strategy committee to assess how well the IT department supports the business strategy.

The other options are not as good as option C. While it is useful to conduct a capability maturity assessment, a customer survey analysis, or an IT controls assurance program, these are not comprehensive enough to evaluate how well the IT department supports the business strategy. They are rather focused on specific

aspects of the IT department, such as its processes, services, or controls. They do not necessarily cover all four perspectives of the IT BSC framework, which provide a holistic view of the IT performance and alignment with the business strategy. Reference := The IT Balanced Scorecard (BSC) Explained - BMC Software1
What Is a Balanced Scorecard (BSC), How Is it Used in Business?2
How to Align Your Business Strategy with Your Technology Strategy …3
How to Measure Your Strategic Plan's Success - dummies
SWOT Analysis: What It Is and When to Use It - Business News Daily How to Communicate Strategy Effectively - ClearPoint Strategy

Question: 223

The MOST effective way to ensure that IT supports the agile needs of an enterprise is to:

A. perform process modeling.
B. outsource infrastructure management.
C. develop a robust enterprise architecture (EA).
D. implement open-source systems.

Answer: C

Explanation:

The MOST effective way to ensure that IT supports the agile needs of an enterprise is to develop a robust enterprise architecture (EA). Enterprise architecture is the practice that supports organizations to understand the complexity of their own business components so they can be changed in a consistent way1. Enterprise architecture provides a framework for change, linked to both strategic direction and business value. It provides organization views to manage complexity,support continuous change, and keep the adequate level of balance between risk and innovation1. Enterprise architecture is also key to support strategic decision making, to provide guidance and guardrails to IT teams that are focused on agile delivery solutions2.
Some of the benefits of developing a robust enterprise architecture for an agile enterprise are3: It aligns the IT objectives and activities with the business strategy and expectations
It enables faster and more effective delivery of IT solutions that meet customer needs and expectations
It reduces waste, duplication, and technical debt by promoting reuse, standardization, and integration of IT assets
It fosters innovation and experimentation by providing a clear vision, direction, and roadmap for new and emerging technologies
It enhances collaboration and communication among stakeholders by providing a common language and understanding of the organization's architecture
Therefore, developing a robust enterprise architecture is the most effective way to ensure that IT supports the agile needs of an enterprise.

Question: 224

Which of the following provides the BEST evidence of effective IT governance?

A. Cost savings and human resource optimization
B. Business value and customer satisfaction
C. IT risk identification and mitigation
D. Comprehensive IT policies and procedures

Answer: B

Explanation:

Effective IT governance is the process of ensuring that IT supports the achievement of the organization's goals and objectives, and delivers value to its stakeholders1. IT governance involves aligning the IT strategy, policies,

processes, and resources with the business strategy, needs, and expectations2. Therefore, the BEST evidence of effective IT governance is business value and customer satisfaction. Business value is the measure of the benefits and outcomes that IT provides to
the organization, such as increased revenue, reduced costs, improved efficiency, enhanced innovation, or competitive advantage3. Customer satisfaction is the measure of the quality and performance of IT services and products, as perceived by the internal and external customers of the organization, such as employees, partners, suppliers, or end-users. By demonstrating business value and customer satisfaction, IT governance can show that IT is aligned with and supports the business goals and objectives.
The other options are not as good as option B. While cost savings and human resource optimization, IT risk identification and mitigation, and comprehensive IT policies and procedures are important aspects of IT governance, they are not sufficient to demonstrateeffective IT governance. They are rather means to achieve the end goal of delivering business value and customer satisfaction. They do not necessarily reflect the extent to which IT supports the achievement of the organization's goals and objectives. Reference :=
What is IT Governance? Definition & Examples | ASQ2
What is IT governance? A formal way to align IT & business strategy1
How to Measure the Value of an IT Investment - TechSoup3
Measuring Customer Satisfaction in Information Technology Services - ISACA

Question: 225

A business is considering a policy to anonymize personal data in enterprise systems. Before making a decision, which of the following is MOST important for the IT steering committee to consider?

A. Business impact analysis (BIA) results
B. Regulatory requirements
C. Sustainability costs to the enterprise
D. Potential implementation barriers

Answer: B

Explanation:

The MOST important thing for the IT steering committee to consider before deciding on a policy to anonymize personal data in enterprise systems is the regulatory requirements. Anonymization is the process of protecting private or sensitive information by erasing or encrypting identifiers that connect an individual to stored data1. However, different jurisdictions may have different definitions, standards, and rules for anonymization and data protection2. For example, the EU's General Data Protection Regulation (GDPR) outlines a specific set of rules that protect user data and create transparency1. The GDPR permits companies to collect anonymized data without consent, use it for any purpose, and store it for an indefinite time—as long as companies remove all identifiers from the data1. However, if the data is not fully anonymized and can be re-identified by using deanonymization methods, then the GDPR still applies and requires consent, purpose limitation, and data minimization2. Therefore, the IT steering committee should consider the regulatory requirements of the applicable legislation in both the home and host countries before deciding on a policy to anonymize personal data in enterprise systems. This can help to ensure compliance, avoid fines or penalties, and protect the reputation and trust of the business.

Question: 226

An enterprise is contracting with an outsourcing partner for a long-term engagement. The BEST time for the enterprise to plan for the event of contract termination is when:

A. planning for the contract as part of business continuity.
B. issues surface in the contractual relationship.
C. developing the initial contract.

D. either party decides to terminate the contract.

Answer: C

Explanation:

The BEST time for the enterprise to plan for the event of contract termination is when developing the initial contract. Contract termination is the process of ending a contractual relationship between two parties, either by mutual agreement or by exercising a right to terminate under the contract terms1. Contract termination can have significant impacts and implications for both parties, such as loss of revenue, loss of service, loss of data, legal disputes, reputational damage, etc.2 Therefore, it is important to plan for the event of contract termination in advance, and include appropriate provisions and mechanisms in the contract to ensure a smooth and orderly exit3.

Some of the benefits of planning for contract termination when developing the initial contract are4: It clarifies the expectations and obligations of both parties in case of contract termination, such as the notice period, the termination fees, the transition services, the data return or destruction, etc. It reduces the risks and costs associated with contract termination, such as service disruption, data loss, litigation, penalties, etc.

It enables faster and more effective resolution of contract termination issues, such as dispute resolution, arbitration, mediation, etc.

It fosters a positive and professional relationship between the parties, even in case of contract termination, by avoiding surprises, conflicts, or misunderstandings.

Therefore, planning for contract termination when developing the initial contract is the best time for the enterprise to ensure a successful and beneficial outsourcing engagement.

Question: 227

The BEST way to decide how to prioritize issues identified in an IT risk and control self-assessment (CSA) is to understand the risk and:

A. impact to the enterprise.
B. criticality of IT services affected.
C. number of IT systems affected.
D. funds required for remediation.

Answer: A

Explanation:

The BEST way to decide how to prioritize issues identified in an IT risk and control self-assessment (CSA) is to understand the risk and the impact to the enterprise. A CSA is a process of identifying, analyzing, and evaluating the potential threats and impacts that could affect the IT objectives, processes, and resources of an organization1. A CSA can help to determine the actions and resources needed to bridge the gaps and achieve the desired outcomes2. To prioritize the issues identified in a CSA, it is important to understand the risk and the impact to the enterprise. The risk is the measure of the likelihood and severity of an adverse event occurring and its consequences on the organization3. The impact is the measure of the extent and magnitude of the harm or damage that an adverse event can cause to the organization, such as financial loss, operational disruption, reputational damage, legal liability, etc.4. By understanding the risk and the impact to the enterprise,

the issues can be prioritized based on their importance and urgency, and the most appropriate and effective solutions can be implemented.

Question: 228

Which of the following is MOST critical to support IT governance cultural changes within an organization?

A. Established IT monitoring and measuring
B. Regularly scheduled governance training
C. Demonstrated management commitment
D. IT governance process manuals

Answer: C

Explanation:

The MOST critical factor to support IT governance cultural changes within an organization is demonstrated management commitment. IT governance is the process of ensuring that IT supports the achievement of the organization's goals and objectives, and delivers value to its stakeholders1. IT governance involves aligning the IT strategy, policies, processes, and resources with the business strategy, needs, and expectations2. However, implementing and sustaining IT governance requires a significant amount of change in the organization, such as introducing new technologies, standards, roles, and responsibilities3. Therefore, demonstrated management commitment is essential for supporting IT governance cultural changes within an organization, as it can: Provide the direction and mandate for the IT governance initiative on an ongoing basis Communicate the vision, mission, goals, and objectives of the IT function to all stakeholders Allocate the necessary resources and capabilities to enable the IT governance processes and activities
Monitor and evaluate the performance and outcomes of the IT function and provide feedback and recognition
Foster a positive and collaborative culture that values IT as a strategic partner and enabler of the business
The other options are not as critical as option C. While it is important to have established IT monitoring and measuring, regularly scheduled governance training, and IT governance process manuals, these are not sufficient to support IT governance cultural changes within an organization. They are rather means to achieve the end goal of implementing and sustaining IT governance. They do not necessarily reflect the level of commitment, involvement, and support from the management toward IT governance.

Question: 229

Which of the following is the PRIMARY purpose of information governance?

A. To develop control procedures that help ensure information is adequately protected throughout its life cycle
B. To monitor the processes that deliver and enhance the value of information assets
C. To set direction for information management capabilities through prioritization and decision making
D. To ensure regulatory compliance is maintained while optimizing the utilization of information

Answer: C

Explanation:

The PRIMARY purpose of information governance is to set direction for information management capabilities through prioritization and decision making. Information governance is the overall strategy for information at an organization. It balances the risk that information presents with the value that information provides1. Information governance helps with legal compliance, operational transparency, and reducing expenditures associated with legal discovery1. To achieve this, information governance requires setting direction for information management capabilities through prioritization and decision making. This involves defining and implementing policies and processes for the effective and efficient acquisition, storage, distribution, usage, and

disposal of information in alignment with business objectives and regulatory requirements2. It also involves ensuring the protection of information quality, integrity, availability, confidentiality, and ownership2. By setting direction for information management capabilities through prioritization and decision making, information governance can help to optimize the value and minimize the risk of information assets. Reference := Information governance - Wikipedia1
What is Information Governance? Why is it Important?3

Question: 230

Communicating which of the following to staff BEST demonstrates senior management's commitment to IT governance?

A. Legal and regulatory requirements
B. Approved IT investment opportunities
C. Objectives and responsibilities
D. Need for enterprise architecture (EA)

Answer: C

Explanation:

Communicating the objectives and responsibilities to staff is the BEST way to demonstrate senior management's commitment to IT governance. IT governance is the process of ensuring that IT supports the achievement of the organization's goals and objectives, and delivers value to its stakeholders1. IT governance involves aligning the IT strategy, policies, processes, and resources with the business strategy, needs, and expectations2. However, implementing and sustaining IT governance requires a significant amount of change in the organization, such as introducing new technologies, standards, roles, and responsibilities3. Therefore, communicating the objectives and responsibilities to staff is essential for demonstrating senior management's commitment to IT governance, as it can:
Provide the direction and mandate for the IT governance initiative on an ongoing basis Communicate the vision, mission, goals, and objectives of the IT function to all stakeholders Allocate the necessary resources and capabilities to enable the IT governance processes and activities
Monitor and evaluate the performance and outcomes of the IT function and provide feedback and recognition
Foster a positive and collaborative culture that values IT as a strategic partner and enabler of the business
The other options are not as good as option C. While it is important to communicate the legal and regulatory requirements, the approved IT investment opportunities, and the need for enterprise architecture (EA), these are not sufficient to demonstrate senior management's commitment to IT governance. They are rather means to achieve the end goal of implementing and sustaining IT governance. They do not necessarily reflect the level of commitment, involvement, and support from the management toward IT governance. Reference :=
What is IT Governance? Definition & Examples | ASQ2
What is IT governance? A formal way to align IT & business strategy1
How to Involve Senior Management in the Information Security Governance …3

Question: 231

Which of the following is the PRIMARY purpose of an effective set of key risk indicators (KRIs)?

A. Identifying possible future adverse impacts on the enterprise
B. Evaluating existing technology for risk monitoring capabilities
C. Establishing executive level buy-in of the risk program
D. Quantifying the productivity of the risk management team

Answer: A

Explanation:

The PRIMARY purpose of an effective set of key risk indicators (KRIs) is to identify possible future adverse impacts on the enterprise. KRIs are metrics or indicators used by organizations to identify, assess, and monitor potential risks. KRIs show how risky a decision, activity, strategy, or plan may be for a business or company. KRIs can be used to monitor operational, technological, financial and staff processes, such as security breaches, economic downturn and staff turnover rate. KRIs are like alarms that alert businesses of changes in the level of risk exposure1. By identifying possible future adverse impacts on the enterprise, KRIs can help to:

Prevent or mitigate the negative consequences of risks, such as financial loss, operational disruption, reputational damage, legal liability, etc.

Enhance the decision-making and planning processes by providing relevant and timely information on risks

Align the risk management activities with the business objectives and expectations Communicate and report the risk status and performance to stakeholders and regulators Therefore, identifying possible future adverse impacts on the enterprise is the primary purpose of an effective set of KRIs.

1: Key Risk Indicators: Examples & Definitions - SolveXia

Question: 232

A multinational enterprise is planning to migrate to cloud-based systems. Which of the following should be of MOST concern to the risk management committee?

A. Cost considerations
B. Regulatory compliance
C. Resource alignment
D. Security breaches

Answer: B

Explanation:

The MOST concerning issue for the risk management committee when planning to migrate to cloud-based systems is regulatory compliance. Regulatory compliance refers to the discipline and process of ensuring that a company follows the laws enforced by governing bodies in their geography or rules required by voluntarily adopted industry standards1. For IT regulatory compliance, people and processes monitor corporate systems to detect and prevent violations ofpolicies and procedures established by these governing laws, regulations, and standards1. However, migrating to cloud-based systems can pose significant challenges and risks for regulatory compliance, such as23:

Data protection, privacy, and sovereignty issues, as cloud service providers may store or process data in different jurisdictions with different legal and regulatory frameworks

Loss of control and visibility over data and systems, as cloud service providers may have different security standards, policies, and practices than the enterprise

Shared responsibility and accountability for compliance, as cloud service providers and customers may have different roles and obligations for ensuring compliance

Complexity and variability of compliance requirements, as cloud service providers may offer different levels of compliance certifications and attestations for different services and regions

Therefore, regulatory compliance should be of most concern to the risk management committee when planning to migrate to cloud-based systems. The risk management committee should carefully assess the compliance requirements of the applicable legislation in both the home and host countries, as well as the compliance capabilities and assurances of the cloud service providers. The risk management committee should also establish appropriate controls and mechanisms to monitor and audit the compliance status and

performance of the cloud-based systems.

Question: 233

An enterprise is planning to outsource data processing for personally identifiable information (PII). When is the MOST appropriate time to define the requirements for security and privacy of information?

A. When issuing requests for proposals (RFPs)
B. After an assessment of the current information architecture.
C. When developing service level agreements (SLAs)
D. During the initial vendor selection process

Answer: A

Explanation:

The requirements for security and privacy of information should be defined when issuing RFPs to ensure that potential vendors can meet the enterprise's expectations and comply with relevant regulations. This will also help the enterprise to evaluate and compare the proposals based on the predefined criteria. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 3: Benefits Realization, Section 3.2: IT Investment Management, Subsection 3.2.2: IT Investment Selection, Page 97-98.

Question: 234

Which of the following is the MOST important aspect of business ethics?

A. Ensuring fair and consistent vendor management practices
B. Providing equal opportunities to employees
C. Protecting stakeholders' interests
D. Complying with legal and regulatory requirements

Answer: C

Explanation:

Business ethics is the study of appropriate business policies and practices regarding potentially controversial subjects, such as corporate governance, insider trading, bribery, discrimination, corporate social responsibility, fiduciary responsibilities, and much more1. The most important aspect of business ethics is to protect the interests of the stakeholders, who are the individuals or groups that have a stake in the success or failure of a business. Stakeholders include shareholders, customers, employees, suppliers, regulators, and the society at large. By protecting stakeholders' interests, a business can ensure its long-term viability, reputation, and profitability. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 1: Governance of Enterprise IT, Section 1.1: IT Governance Frameworks and Principles, Subsection 1.1.2: IT Governance Principles, Page 14-15. Business Ethics: Definition, Principles, Why They're Important.

Question: 235

Which of the following is the BEST way to ensure all enterprise employees understand the corporate code of business conduct?

A. Conduct scheduled and random compliance audits.
B. Mandate annual ethics training that includes an exam.
C. Require external business activities be documented and reported.
D. Distribute a copy of the code and require a signature.

Answer: B

Explanation:

The best way to ensure all enterprise employees understand the corporate code of business conduct is to mandate annual ethics training that includes an exam. This will help employees to learn the content and principles of the code, as well as test their knowledge and comprehension. Ethics training can also reinforce the importance of ethical behavior and the consequences of violating the code. According to a Harvard Business Review article1, ethics training can help employees to develop ethical skills, such as moral awareness, moral reasoning, moral courage, and moral leadership1. A code of conduct is not effective if employees do not know or understand it, or if they do not apply it in their daily work. Therefore, ethics training is essential to ensure employees are aware of and adhere to the corporate code of business conduct. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 1: Governance of Enterprise IT, Section 1.1: IT Governance Frameworks andPrinciples, Subsection 1.1.2: IT Governance Principles, Page 1415. Building an Ethical Company.

Question: 236

A major data leakage incident at an enterprise has resulted in a mandate to strengthen and enforce current data governance practices. Which of the following should be done FIRST to achieve this objective?

A. Assess data security controls.
B. Review data logs.
C. Analyze data quality.
D. Verify data owners.

Answer: D

Explanation:

The first step to strengthen and enforce current data governance practices after a data leakage incident is to verify data owners. Data owners are the individuals or groups who have the authority and responsibility to define, classify, protect, and manage the data assets of an enterprise1. By verifying data owners, the enterprise can ensure that the data is properly accounted for, categorized, and secured according to its value, sensitivity, and risk. Data owners can also establish data policies, standards, and procedures, as well as monitor and report on data quality, usage, and compliance1. Verifying data owners is a prerequisite for assessing data security controls, reviewing data logs, and analyzing data quality, as these activities depend on the accurate identification and assignment of data ownership roles and responsibilities. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 4: Risk Optimization, Section 4.2: IT Risk Management Process, Subsection 4.2.1: IT Risk Identification, Page 163-164. Top 10 Effective Data Governance Tools.

Question: 237

A newly hired CIO has been told the enterprise has an established IT governance process, but finds it is not being followed. To address this problem, the CIO should FIRST

A. gain an understanding of the existing governance process and corporate culture.
B. replace the current governance process with one the CIO has successfully used before.
C. establish personal relationships with executive-level peers to leverage goodwill,
D. engage audit to review current governance processes and validate the ClO's concerns.

Answer: A

Explanation:

The first step for the newly hired CIO to address the problem of IT governance process not being followed is to gain an understanding of the existing governance process and corporateculture. This will help the CIO to identify the root causes of the problem, such as lack of awareness, commitment, alignment, communication, or

accountability. It will also help the CIO to assess the strengths and weaknesses of the current process, as well as the opportunities and threats for improvement. By understanding the existing governance process and corporate culture, the CIO can also build trust and rapport with the stakeholders, and tailor the solutions to fit the specific needs and context of the enterprise. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 1: Governance of Enterprise IT, Section 1.2: IT Governance Implementation, Subsection 1.2.1: IT Governance Implementation Process, Page 27-28. What is CGEIT? A certification for seasoned IT governance professionals.

Question: 238

Which of the following should be the FIRST step in updating an IT strategic plan?

A. Revise the enterprise architecture (EA).
B. Review IT performance objectives and indicators.
C. Evaluate IT capabilities and resources.
D. Identify changes in enterprise goals.

Answer: D

Explanation:

The first step in updating an IT strategic plan is to identify changes in enterprise goals. An IT strategic plan is a document that defines how the IT function supports the overall business strategy and objectives of an enterprise1. It should be aligned with and driven by the enterprise goals, which may change over time due to internal or external factors, such as market conditions, customer demands, competitor actions, regulatory requirements, or organizational changes2. Therefore, before updating the IT strategic plan, it is essential to identify and understand the changes in enterprise goals and their implications for IT. This will help to ensure that the IT strategic plan remains relevant, realistic, and effective in delivering value to the enterprise. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 2: IT Resources, Section 2.1: IT Strategy Development and Maintenance, Subsection 2.1.1: IT Strategy Development Process, Page 5556. What is an IT Strategic Plan?.

Question: 239

Which of the following would be MOST useful for prioritizing IT improvement initiatives to achieve desired business outcomes?

A. Budget variance analysis
B. Enterprise architecture (EA)
C. IT skills matrix
D. Portfolio management

Answer: D

Explanation:

Portfolio management is the most useful technique for prioritizing IT improvement initiatives to achieve desired business outcomes. Portfolio management is the process of selecting, prioritizing, balancing, and monitoring the IT investments and initiatives that support the enterprise's strategic objectives and deliver value to the stakeholders1. Portfolio management helps to align IT with business goals, optimize resource allocation, manage risks and dependencies, and measure performance and benefits1. By applying portfolio management, an enterprise can ensure that the IT improvement initiatives are consistent with its vision, mission, values, and priorities, and that they contribute to the desired business outcomes1. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 3: Benefits Realization,

Section 3.1: IT Portfolio Management, Page 83-84. What is IT portfolio management? A framework for aligning technology and business.

Question: 240

Which of the following is the BEST method to confirm whether a pilot project was successful?

A. Determine whether the pilot aligns with the as-is enterprise architecture (EA).
B. Evaluate whether the pilot project achieved planned schedule and cost.
C. Assess the results of the pilot project against the expected performance outcomes.
D. Review the metrics recorded in the IT balanced scorecard.

Answer: C

Explanation:

The best method to confirm whether a pilot project was successful is to assess the results of the pilot project against the expected performance outcomes. A pilot project is a small-scale experiment that tests the feasibility, effectiveness, and scalability of a new idea, process, product, or service before implementing it on a larger scale12. The purpose of a pilot project is to validate the assumptions, identify the risks and issues, and measure the benefits and costs of the proposed solution12. Therefore, to determine the success of a pilot project, it is essential to compare the actual results with the expected outcomes that were defined at the beginning of the pilot project12. These outcomes should be based on specific, measurable, achievable, relevant, and timebound (SMART) criteria that reflect the objectives and value proposition of the solution12. By assessing the results of the pilot project against the expected performance outcomes, an enterprise can evaluate whether the pilot project met its goals, delivered value to the stakeholders, and proved its viability for scaling up

Question: 241

The CIO of a large enterprise has taken the necessary steps to align IT objectives with business objectives. What is the BEST way for the CIO to ensure these objectives are delivered effectively by IT staff?

A. Map the IT objectives to an industry-accepted framework.
B. Enhance Ihe budget for training based on the IT objectives.
C. Include the IT objectives in staff performance plans.
D. Include CIO sign-off of the objectives as part of the IT strategic plan.

Answer: C

Explanation:

The best way for the CIO to ensure that the IT objectives are delivered effectively by IT staff is to include the IT objectives in staff performance plans. Staff performance plans are documents that define the expectations, responsibilities, and goals for individual employees, as well as the criteria and methods for evaluating their performance1. By including the IT objectives in staff performance plans, the CIO can align the IT staff's work with the business objectives, communicate the desired outcomes and behaviors, motivate and empower the IT staff, monitor and measure their progress and achievements, and provide feedback and recognition1. This will help to create a culture of accountability, excellence, and continuous improvement among the IT staff, and ensure that they contribute to the value creation and delivery of IT2. Reference: Performance Management. What is CGEIT? A certification for seasoned IT governance professionals.

Question: 242

The CIO of a large enterprise has taken the necessary steps to align IT objectives with business objectives. What is the BEST way for the CIO to ensure these objectives are delivered effectively by IT staff?

A. Map the IT objectives to an industry-accepted framework.
B. Enhance the budget for training based on the IT objectives.
C. Include the IT objectives in staff performance plans.
D. Include CIO sign-off of the objectives as part of the IT strategic plan.

Answer: C

Explanation:

This is the best way for the CIO to ensure that the IT objectives are delivered effectively by IT staff, as it aligns their work with the business objectives, communicates the desired outcomes and behaviors, motivates and empowers them, monitors and measures their progress and achievements, and provides feedback and recognition1. This answer is supported by the CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 2: IT Resources, Section 2.1: IT Strategy Development and Maintenance, Subsection 2.1.3: IT Strategy Implementation, Page 64-65. It is also confirmed by a CIO article that states that "including the IT objectives in staff performance plans" is one of the best practices for aligning IT with business goals1. The other options are not as effective as option C, as they do not directly link the IT objectives with the IT staff's performance and incentives. Option A may helpto standardize and benchmark the IT objectives, but it does not ensure that they are delivered by the IT staff. Option B may help to improve the IT staff's skills and knowledge, but it does not ensure that they are aligned with the IT objectives. Option D may help to demonstrate the CIO's commitment and authority, but it does not ensure that the IT staff are aware of and adhere to the IT objectives.

Question: 243

An IT manager is trying to determine optimal IT service levels. Which of the following should be the PRIMARY consideration?

A. Internal rate of return
B. Recovery time objective (RTO)
C. Cost-benefit analysis
D. Resource utilization analysis

Answer: C

Explanation:

The primary consideration for determining optimal IT service levels is cost-benefit analysis. Costbenefit analysis is a technique that compares the costs and benefits of providing a certain level of IT service to the business and the stakeholders1. It helps to identify the optimal balance between the value and the cost of IT service delivery, and to justify the investment and resources required for achieving the desired service level objectives1. Cost-benefit analysis can also help to evaluate alternative options, prioritize improvement initiatives, and measure the return on investment of IT service management1. The other options are not as relevant as cost-benefit analysis, as they do not consider both the costs and benefits of IT service levels. Internal rate of return is a financial metric that measures the profitability of an investment, but it does not account for the non-financial benefits or risks of IT service delivery2. Recovery time objective is a parameter that specifies the maximum acceptable time for restoring an IT service after a disruption, but it does not reflect the cost or value of achieving that time3. Resource utilization analysis is a technique that monitors and optimizes the usage and allocation of IT resources, but it does not assess the impact or outcome of IT service delivery on the business and the stakeholders4. Reference: Cost-Benefit Analysis in IT Service Management. Internal Rate of Return (IRR). Recovery Time Objective (RTO). Resource Utilization Analysis.

Question: 244

The board of directors of a large organization has directed IT senior management to improve IT governance within the organization. IT senior management's MOST important course of action should be to:

A. understand the driver that led to a desire to change.
B. assess the current slate of IT governance within the organization.
C. review IT strategy and direction.
D. analyze IT service levels and performance.

Answer: A

Explanation:

The most important course of action for IT senior management to improve IT governance within the organization is to understand the driver that led to a desire to change. IT governance is the process of ensuring that IT supports and enables the achievement of the enterprise's goals and objectives, and delivers value to the stakeholders1. IT governance is influenced by various internal and external factors, such as business strategy, customer expectations, regulatory requirements, industry standards, best practices, and emerging technologies1. Therefore, before initiating any improvement initiatives, IT senior management should first identify and analyze the driver that prompted the board of directors to request a change in IT governance. This will help them to understand the current situation, the desired state, the gap between them, and the rationale and urgency for improvement2. By understanding the driver that led to a desire to change, IT senior management can also align their improvement efforts with the board's vision and expectations, communicate the benefits and challenges of change, and gain their support and commitment2. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 1: Governance of Enterprise IT, Section 1.1: IT Governance Frameworks and Principles, Page 9-10. What is CGEIT? A certification for seasoned IT governance professionals.

Question: 245

When assessing the impact of a new regulatory requirement, which of the following should be the FIRST course of action?

A. Update affected IT policies.
B. Assess the budget impact of the new regulation.
C. Map the regulation to business processes.
D. Implement new regulatory requirements.

Answer: C

Explanation:

The first course of action when assessing the impact of a new regulatory requirement is to map the regulation to business processes. This means identifying and analyzing which business processes are affected by the new regulation, how they are affected, and what changes are needed to comply with the regulation1. Mapping the regulation to business processes helps to understand the scope, complexity, and priority of the regulatory compliance project, and to align the IT and business objectives and strategies1. It also helps to identify the stakeholders, roles, responsibilities, and risks involved in the compliance process, and to communicate and coordinate with them effectively1. The other options are not as important as mapping the regulation to business processes, as they are dependent on the outcome of this step. Updatingaffected IT policies, assessing the budget impact of the new regulation, and implementing new regulatory requirements are subsequent steps that should be done after mapping the regulation to business processes2. Reference: How to Map Regulations to Business Processes. CGEIT Certification | Certified in Governance of Enterprise IT | ISACA.

Question: 246

An IT strategy committee has reviewed an audit report indicating sales employees are using personal smartphones to conduct corporate business. Although the committee appreciates the business benefits, it is also concerned with the security risk. To deliver the business benefit, what should be the committee's FIRST recommendation?

A. Document procedures for securing personal devices.
B. Improve training courses on securing corporate information.
C. Perform a risk assessment on personal device data protection.
D. Update the corporate security policy to include personal devices.

Answer: C

Explanation:

This should be the committee's first recommendation, as it will help to identify and evaluate the potential threats, vulnerabilities, and impacts of using personal smartphones to conduct corporate business1. A risk assessment will also help to determine the appropriate controls and mitigation strategies to protect the corporate information and assets, as well as comply with the relevant regulations and standards1. The other options are not as important as performing a risk assessment, as they are dependent on the outcome of this step. Documenting procedures for securing personal devices, improving training courses on securing corporate information, and updating the corporate security policy to include personal devices are possible actions that may be taken after performing a risk assessment, based on the identified risks and their levels2.

Question: 247

An enterprise has made the strategic decision to reduce operating costs for the next year and is taking advantage of cost reductions offered by an external cloud service provider. Which of the following should be the IT steering committee's PRIMARY concern?

A. Calculating the cost of the current solution
B. Updating the business risk profile
C. Changing the IT steering committee charter
D. Revising the business's balanced scorecard

Answer: B

Explanation:

This should be the IT steering committee's primary concern, as moving to an external cloud service provider may introduce new or different risks to the enterprise, such as data security,privacy, compliance, availability, performance, vendor lock-in, and service level agreements12. The IT steering committee should update the business risk profile to reflect the current and potential risks associated with the cloud service provider, and to ensure that they are aligned with the enterprise's risk appetite and tolerance12. The IT steering committee should also monitor and manage the risks throughout the cloud service lifecycle, and implement appropriate controls and mitigation strategies to protect the enterprise's assets and interests12. The other options are not as important as updating the business risk profile, as they are not directly related to the strategic decision to reduce operating
costs for the next year. Calculating the cost of the current solution, changing the IT steering committee charter, and revising the business's balanced scorecard are possible actions that may be taken after updating the business risk profile, based on the identified risks and their levels3.

Question: 248

Which of the following should be the PRIMARY goal of implementing an IT strategic planning process?

A. Determining benefits from IT deployments
B. Optimizing IT resources to drive innovation
C. Directing business strategy to achieve goals
D. Translating business needs into IT initiatives

Answer: D

Explanation:

Translating business needs into IT initiatives. IT strategic planning is the process of defining how the IT function supports and enables the overall business strategy and objectives of an enterprise1. It helps to align IT with business goals, optimize IT investments and resources, manage IT risks and opportunities, and deliver value to the stakeholders1. By implementing an IT strategic planning process, an enterprise can translate its business needs into IT initiatives that are consistent, coherent, and feasible1. These IT initiatives can include projects, programs, services, systems, architectures, policies, standards, and processes that address the current and future business requirements and challenges1. Translating business needs into IT initiatives is the primary goal of implementing an IT strategic planning process, as it ensures that IT is responsive, relevant, and effective in supporting the enterprise's mission, vision, and values1.

Question: 249

A health tech enterprise wants to ensure that its in-house developed mobile app for users complies with data privacy regulations. Which of the following should be identified FIRST when creating an inventory of information systems and data related to the mobile app?

A. Data maintained by vendors
B. Vendors and outsourced systems
C. Application and data owners
D. Information classification scheme

Answer: C

Explanation:

This should be identified first when creating an inventory of information systems and data related to the mobile app, as they are the individuals or groups who have the authority and responsibility to define, classify, protect, and manage the data assets of the enterprise1. By identifying the application and data owners, the enterprise can ensure that the data is properly accounted for, categorized, and secured according to its value, sensitivity, and risk. Application and data owners can also establish data policies, standards, and procedures, as well as monitor and report on data quality, usage, and compliance1. Identifying the application and data owners is a prerequisite for identifying the other options, such as data maintained by vendors, vendors and outsourced systems, and information classification scheme, as these depend on the accurate identification and assignment of
data ownership roles and responsibilities.

Question: 250

An enterprise wants to address the human factors of social engineering risk within the organization. From a governance perspective, which of the following is the BEST way to mitigate this risk?

A. Distribute the social media information security policy to staff.
B. Mandate annual security awareness training.

C. Restrict access to social media.
D. Mandate security requirements be included in employee contracts.

Answer: B

Explanation:

This is the best way to mitigate the human factors of social engineering risk within the organization from a governance perspective, as it helps to educate and empower the employees to recognize and prevent social engineering attacks. Social engineering attacks are malicious attacks that use deception and manipulation to exploit human behavior and trick people into revealing sensitive information, clicking malicious links, or opening malicious files1. These attacks can cause serious damage to the organization, such as financial loss, data breach, reputation harm, or legal liability1. Therefore, it is essential to address the human factors of social engineering risk, which are the psychological and emotional vulnerabilities that make people susceptible to these attacks, such as curiosity, greed, fear, urgency, or trust2. By mandating annual security awareness training, the organization can raise the level of knowledge and awareness among the employees about the common types, techniques, and indicators of social engineering attacks, as well as the best practices and policies to avoid them2. Security awareness training can also help to foster a culture of security and responsibility among the employees, and to reinforce their role and accountability in protecting the organization's assets and interests2. The other options are not as effective as mandating annual security awareness training, as they do not address the human factors of social engineering risk directly. Distributing the social media information security policy to staff may help to inform them about the rules and expectations for using social media platforms, but it does not ensure that they understand or follow them. Restricting access to social media may help to reduce the exposure to potential social engineering attacks, but it does not prevent them from occurring through other channels or mediums. Mandating security requirements be included in employee contracts may help to enforce compliance and deter violations, but it does not prevent them from happening due to ignorance or negligence.

Question: 251

Which of the following has the GREATEST influence on data quality assurance?

A. Data stewardship
B. Data encryption
C. Data classification
D. Data modeling

Answer: A

Explanation:

Data stewardship is the process of defining, implementing, and enforcing policies, standards, roles, and responsibilities for the quality, security, privacy, and usage of data within an enterprise1. Data stewardship has the greatest influence on data quality assurance, as it ensures that the data is accurate, complete, consistent, timely, and fit for its intended purpose1. Data stewardship also helps to identify and resolve data quality issues, monitor and measure data quality performance, and improve data quality over time1. The other options are not as influential as data stewardship, as they are specific aspects or techniques of data management, but not comprehensive processes. Data encryption is the process of transforming data into an unreadable format to protect it from unauthorized access or modification2. Data encryption can enhance data security and privacy, but it does not directly affect data quality assurance. Data classification is the process of categorizing data based on its value, sensitivity, and risk to the enterprise. Data classification can help to apply appropriate controls and policies for data protection and compliance, but it does not directly affect data quality assurance. Data modeling is the process of creating a representation of the structure, relationships, and

meaning of data within a specific domain or context. Data modeling can help to design and optimize databases and applications that use data, but it does not directly affect data quality assurance.

Question: 252

Which of the following is MOST important to consider when planning to implement a cloud-based application for sharing documents with internal and external parties?

A. Cloud implementation model
B. User experience
C. Information ownership
D. Third-party access rights

Answer: C

Explanation:

Information ownership is the right and responsibility to define, classify, protect, and manage the data assets of an enterprise. When using a cloud-based application, the enterprise should ensure that it retains the ownership and control of its information, and that it complies with the relevant laws and regulations regarding data privacy, security, and sovereignty12. The enterprise should also establish clear policies and agreements with the cloud service provider and the internal and external parties regarding the access, usage, storage, transfer, retention, and disposal of the information12. By considering information ownership, the enterprise can mitigate the risks and challenges of using a cloud-based application, such as data breaches, unauthorized access, vendor lock-in, legal disputes, or reputational damage12.

The other options are not as important as information ownership, as they are secondary or dependent factors. Cloud implementation model is the type of cloud service that the enterprise chooses to use, such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS)3. Cloud implementation model can affect the cost, performance, scalability, and flexibility of the cloud-based application, but it does not directly affect the ownership and governance of the information3. User experience is the perception and satisfaction of the users when interacting with the cloud-based application. User experience can affect the adoption, engagement, and productivity of the users, but it does not directly affect the ownership and governance of the information. Third-party access rights are the permissions and restrictions that the enterprise grants to external parties to access and use its information through the cloud-based application. Third-party access rights can affect the security and privacy of the information, but they are determined by the information ownership policies and agreements that the enterprise
establishes with the cloud service provider and the external parties12.

Question: 253

In an enterprise that has worldwide business units and a centralized financial control model, which of the following is a barrier to strategic alignment of business and IT?

A. Each business unit has its own steering committee for IT investment and prioritization.
B. Uniform portfolio management is in place throughout the business units.
C. IT is the exclusive provider of IT services to the business units.
D. The enterprise's CIO is a member of the executive committee.

Answer: A

Explanation:

This is a barrier to strategic alignment of business and IT, as it creates inconsistency and fragmentation in the IT governance process across the enterprise. Strategic alignment of business and IT is the degree of fit and

integration among business strategy, IT strategy, business infrastructure, and IT infrastructure1. It helps to ensure that IT supports and enables the achievement of the enterprise's goals and objectives, and delivers value to the stakeholders1. To achieve strategic alignment, an enterprise needs to have a coherent and coordinated IT governance process that aligns IT with business goals, optimizes IT investments and resources, manages IT risks and opportunities, and measures IT performance and benefits1. However, if each business unit has its own steering committee for IT investment and prioritization, this may result in conflicting or competing IT priorities, duplication or waste of IT resources, lack of communication or collaboration among IT stakeholders, or misalignment of IT services and capabilities with business needs and expectations1. Therefore, each business unit having its own steering committee for IT investment and prioritization is a barrier to strategic alignment of business and IT.

The other options are not barriers to strategic alignment of business and IT, as they are possible enablers or indicators of strategic alignment. Uniform portfolio management is the process of selecting, prioritizing, balancing, and monitoring the IT investments and initiatives that support the enterprise's strategic objectives and deliver value to the stakeholders2. Uniform portfolio management can help to align IT with business goals, optimize resource allocation, manage risks and dependencies, and measure performance and benefits2. IT being the exclusive provider of IT services to the business units can help to ensure that the IT services are consistent, reliable, secure, and compliant with the enterprise's standards and policies3. The enterprise's CIO being a member of the executive committee can help to demonstrate the strategic importance and contribution of IT to the enterprise's success, as well as facilitate the communication and collaboration between IT and business leaders4.

Question: 254

An enterprise's executive team has recently released a new IT strategy and related objectives. Which of the following would be the MOST effective way for the CIO to ensure IT personnel are supporting the new strategy's objectives?

A. Measure progress towards IT objectives and communicate the results to IT staff.
B. Incorporate IT objectives into individual performance evaluations.
C. Develop communication materials to promote the new IT strategy and objectives.
D. Require IT managers to assign activities aligned to the IT objectives.

Answer: B

Explanation:

This way, the CIO can align the IT personnel's work with the new strategy's objectives, communicate the desired outcomes and behaviors, motivate and empower the IT personnel, monitor and measure their progress and achievements, and provide feedback and recognition1. Incorporating IT objectives into individual performance evaluations can also create a culture of accountability, excellence, and continuous improvement among the IT personnel, and ensure that they contribute to the value creation and delivery of IT2.

The other options are not as effective as incorporating IT objectives into individual performance evaluations, as they do not directly link the IT objectives with the IT personnel's performance and incentives. Measuring progress towards IT objectives and communicating the results to IT staff may help to inform them about the status and direction of the new strategy, but it does not ensure that they understand or follow it. Developing communication materials to promote the new IT strategy and objectives may help to raise awareness and interest among the IT staff, but it does not ensure that they adopt or support it. Requiring IT managers to assign activities aligned to the IT objectives may help to implement the new strategy at the operational level, but it does not ensure that the IT staff are engaged or committed to it.

Question: 255

The PRIMARY reason for using quantitative criteria in developing business cases for IT projects is to:

A. improve the process of evaluating returns after implementation.

B. benchmark project success with similar enterprises.
C. learn lessons from errors made in past projects.
D. apply other corporate standards to the development project.

Answer: A

Explanation:

Quantitative criteria are measurable and objective indicators that can be used to assess the costs, benefits, risks, and value of IT projects1. By using quantitative criteria, an enterprise can compare and prioritize different IT project proposals, justify and secure the required funding and resources, monitor and control the project progress and performance, and evaluate the actual outcomes and impacts of the project after implementation1. Quantitative criteria can also help to demonstrate the alignment of IT projects with the enterprise's strategic objectives and goals, and to communicate the value proposition of IT projects to the stakeholders1.

The other options are not the primary reason for using quantitative criteria in developing business cases for IT projects, as they are either secondary or unrelated benefits. Benchmarking project success with similar enterprises may help to identify best practices and areas for improvement, but it is not the main purpose of using quantitative criteria. Learning lessons from errors made in past projects may help to avoid repeating mistakes and enhance project quality, but it is not the main purpose of using quantitative criteria. Applying other corporate standards to the development project may help to ensure consistency and compliance, but it is not the main purpose of using quantitative criteria.

Question: 256

Which of the following is the MOST important reason to include internal audit as a stakeholder when establishing clear roles for the governance of IT?

A. Internal audit has knowledge and technical expertise to advise on IT infrastructure.
B. Internal audit is accountable for the overall enterprise governance of IT.
C. Internal audit implements controls over IT risks and security.
D. Internal audit provides input on relevant issues and control processes.

Answer: D

Explanation:

Internal audit is an independent and objective function that provides assurance and consulting services to the enterprise on the effectiveness and efficiency of its governance, risk management,and control processes1. By including internal audit as a stakeholder, the enterprise can benefit from its knowledge, expertise, and perspective on IT-related issues and risks, such as IT strategy alignment, IT performance measurement, IT value delivery, IT resource management, IT risk management, and IT compliance2. Internal audit can also provide input on the design, implementation, and evaluation of the IT governance framework, policies, standards, and procedures, as well as recommend improvements and best practices2. Therefore, internal audit provides input on relevant issues and control processes, which is the most important reason to include it as a stakeholder when establishing clear roles for the governance of IT.

The other options are not as important or accurate as option D. Internal audit does not have knowledge and technical expertise to advise on IT infrastructure, as this is not its primary role or responsibility. Internal audit is not accountable for the overall enterprise governance of IT, as this is the responsibility of the board of directors and senior management3. Internal audit does not implement controls over IT risks and security, as this is the responsibility of the IT function and other business units4.

Question: 257

When developing an IT governance framework, it is MOST important for an enterprise to consider:

A. information technology risk.
B. framework development cost.
C. information technology strategy.
D. stakeholders' support.

Answer: D

Explanation:

IT governance is the process of ensuring that IT supports and enables the achievement of the enterprise's goals and objectives, and delivers value to the stakeholders1. Stakeholders are the individuals or groups that have a stake in the success or failure of IT governance, such as board members, senior management, business units, IT function, customers, suppliers, regulators, and society1. By considering stakeholders' support, an enterprise can ensure that the IT governance framework is aligned with and driven by the stakeholders' needs, expectations, and interests1. Stakeholders' support can also help to facilitate the communication, collaboration, and decision-making processes among the IT governance participants, and to gain their commitment and buy-in for the IT governance implementation and improvement1.

The other options are not as important as stakeholders' support, as they are either specific aspects or outcomes of IT governance, but not comprehensive factors. Information technology risk is the potential for negative consequences due to the use or misuse of IT within an enterprise. Information technology risk can affect the IT governance framework, but it is not the most important factor to consider, as it is only one of the many elements that influence ITgovernance2. Framework development cost is the amount of money and resources required to design and implement the IT governance framework. Framework development cost can affect the IT governance framework, but it is not the most important factor to consider, as it is only one of the many criteria that evaluate IT governance3. Information technology strategy is the plan that defines how the IT function supports and enables the overall business strategy and objectives of an enterprise. Information technology strategy can affect the IT governance framework, but it is not the most important factor to consider, as it is only one of the many components that constitute IT governance

Question: 258

To ensure that information can be traced to the originating event and accountable parties, an enterprise should FIRST:

A. capture source information and supporting evidence.
B. improve business process controls.
C. review information event logs tor potential incidents.
D. review retention requirements for source information.

Answer: A

Explanation:

This should be the first step to ensure that information can be traced to the originating event and accountable parties, as it helps to establish the authenticity, integrity, and reliability of the information. Source information and supporting evidence are the data and documents that provide the context, details, and proof of an information event, such as who, what, when, where, why, and how1. By capturing source information and supporting evidence, an enterprise can link the information to its source and originator, verify its accuracy and completeness, and identify its owner and custodian1. Capturing source information and supporting evidence

can also help to comply with the legal and regulatory requirements for information traceability, such as data protection, privacy, audit, and e-discovery2. Capturing source information and supporting evidence is a prerequisite for the other options, such as improving business process controls, reviewing information event logs for potential incidents, and reviewing retention requirements for source information, as these activities depend on the availability and quality of the source information and supporting evidence.

Question: 259

An enterprise has developed a new digital strategy to improve fraud detection. Which of the following is MOST important to consider when updating the information architecture?

A. Resource constraints related to implementing the digital strategy.
B. The business use cases supporting the digital strategy
C. Changes to the legacy business and data architectures
D. The history of fraud incidents and their root causes

Answer: B

Explanation:

Business use cases are descriptions of the business processes, scenarios, and interactions that support the achievement of a specific business goal or objective1. By considering the business use cases supporting the digital strategy, the enterprise can ensure that the information architecture is aligned with and driven by the business needs and expectations2. The information architecture can also support the communication, collaboration, and decision-making processes among the stakeholders involved in the digital strategy2.

The other options are not as important as the business use cases supporting the digital strategy, as they are either specific aspects or outcomes of information architecture, but not comprehensive factors. Resource constraints related to implementing the digital strategy are the limitations and challenges that affect the availability and quality of the resources required for executing the digital strategy, such as time, money, people, technology, or data3. Resource constraints can affect the information architecture, but they are not the most important factor to consider, as they are only one of the many criteria that evaluate information architecture3. Changes to the legacy business and data architectures are the modifications and adaptations that are needed to update and improve the existing business and data structures, models, and systems to align with the digital strategy4. Changes to the legacy business and data architectures can affect the information architecture, but they are not the most important factor to consider, as they are only one of the many components that constitute information architecture4. The history of fraud incidents and their root causes are the records and analyses of the previous fraud events and their underlying factors that occurred within or against the enterprise5. The history of fraud incidents and their root causes can affect the information architecture, but they are not the most important factor to consider, as they are only one of the many sources of information that inform information architecture5.

Question: 260

A software company's products have had significant quality issues in recent releases. As a result, market reputation and customer satisfaction ratings have been suffering. What should executive leadership do FIRST to address this concern?

A. Allocate budget to hire more software and quality assurance specialists
B. Implement a software development life cycle (SDLC) framework.
C. Mandate more robust software testing prior to release.
D. Require a root cause analysis and review results.

Answer: D

Explanation:

This should be the first thing that executive leadership does to address the concern of quality issues in their software products, as it helps to identify and understand the underlying factors and causes that led to the quality problems1. A root cause analysis is a systematic process of investigating a problem or incident by asking a series of questions, such as why, how, what, where, and when, until the root cause or causes are found1. By requiring a root cause analysis and reviewing the results, executive leadership can gain insight into the nature and extent of the quality issues, as well as their impact on the market reputation and customer satisfaction ratings. They can also use the results to devise and implement corrective and preventive actions to resolve the quality issues and prevent them from recurring1.

The other options are not as important or effective as requiring a root cause analysis and reviewing the results, as they are either specific solutions or outcomes of the root cause analysis, but not comprehensive steps. Allocating budget to hire more software and quality assurance specialists may help to improve the software development and testing process, but it may not address the root cause or causes of the quality issues, which could be related to other factors, such as requirements, design,
tools, methods, or culture2. Implementing a software development life cycle (SDLC) framework may help to standardize and optimize the software development process, but it may not address the root cause or causes of the quality issues, which could be related to other factors, such as communication, collaboration, feedback, or training3. Mandating more robust software testing prior to release may help to detect and fix more defects before launching the software products, but it may not address the root cause or causes of the quality issues, which could be related to other factors, such as scope creep, change management, or quality assurance

Question: 261

An enterprise's board of directors has determined that IT is not sufficiently supporting its corporate objectives, and has established a committee to address this problem. Which of the following should be the committees FIRST action?

A. Implement a continuous improvement plan.
B. Specify IT human resource performance measures.
C. Create an IT strategic plan.
D. Develop a service level management plan.

Answer: C

Explanation:

This should be the committee's first action, as it will help to define how the IT function supports and enables the overall business strategy and objectives of the enterprise1. An IT strategic plan is a document that outlines the vision, mission, goals, and initiatives of the IT function, as well as the resources, processes, and metrics required to achieve them1. By creating an IT strategic plan, the committee can align IT with business needs and expectations, optimize IT investments andresources, manage IT risks and opportunities, and deliver value to the stakeholders1. Creating an IT strategic plan can also help to communicate and demonstrate the role and contribution of IT to the enterprise's success, and to gain the support and commitment of the board of directors and senior management1.

The other options are not as important or effective as creating an IT strategic plan, as they are either specific solutions or outcomes of the IT strategic plan, but not comprehensive steps. Implementing a continuous improvement plan may help to enhance the quality and efficiency of IT services and processes, but it may not address the root cause or causes of IT not sufficiently supporting the corporate objectives, which could be

related to other factors, such as strategy alignment, value delivery, resource management, or risk optimization2. Specifying IT human resource performance measures may help to evaluate and improve the skills and productivity of IT staff, but it may not address the root cause or causes of IT not sufficiently supporting the corporate objectives, which could be related to other factors, such as stakeholder engagement, communication, collaboration, or feedback3. Developing a service level management plan may help to define and monitor the expectations and agreements for IT service delivery between IT providers and customers, but it may not address the root cause or causes of IT not sufficiently supporting the corporate objectives, which could be related to other factors, such as business requirements, customer satisfaction, innovation, or agility.

Question: 262

The CEO of an organization is concerned that there are inconsistencies in the way information assets are classified across the enterprise. Which of the following is be the BEST way for the CIO to address these concerns?

A. Include data assets in the IT inventory.
B. Identify data owners across the enterprise.
C. Require enterprise risk assessments.
D. Implement enterprise data governance.

Answer: D

Explanation:

Enterprise data governance is a system for defining who within an organization has authority and control over data assets and how those data assets may be used. It encompasses the people, processes, and technologies required to manage and protect data assets1. Enterprise data governance can help address the inconsistencies in data classification by establishing a common framework, standards, and policies for data quality, security, and usage across the enterprise. It can also assign roles and responsibilities for data owners, stewards, and custodians to ensure accountability and compliance234. Reference:

2: https://www.ibm.com/topics/data-governance
1: https://www.cio.com/article/202183/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html
3: https://www.sailpoint.com/identity-library/enterprise-data-governance/
4: https://atlan.com/enterprise-data-governance/

Question: 263

The PRIMARY objective of promoting business ethics within the IT enterprise should be to ensure:

A. trust among internal and external stakeholders.
B. employees act more responsibly.
C. corporate social responsibility.
D. legal and regulatory compliance.

Answer: A

Explanation:

Business ethics is the application of ethical values to business behaviour. It encompasses the people, processes, and technologies required to manage and protect data assets1. Promoting business ethics within the IT enterprise should be the primary objective because it ensures trust among internal and external stakeholders, such as customers, employees, suppliers, regulators, and society234. Trust is important because it makes cooperation possible, enhances performance, fosters engagement, and creates long-term value21. While the other options are also desirable outcomes of business ethics, they are not the primary objective. Employees acting more responsibly, corporate social responsibility, and legal and regulatory compliance are all

consequences of trust-building rather than the main goal. Reference:

2: https://www.ibm.com/topics/data-governance

1: https://www.cio.com/article/202183/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html

3: https://www.sailpoint.com/identity-library/enterprise-data-governance/

4: https://atlan.com/enterprise-data-governance/

Question: 264

The PRIMARY reason for periodically evaluating IT resource staffing requirements is to:

A. ascertain the IT function has sufficient skilled staff to maintain daily operations.
B. ensure the enterprise has sufficient resources to address changing business and IT needs.
C. verify that human resource recruitment and retention processes meet enterprise IT objectives.
D. confirm IT-related responsibilities are defined for the enterprise's business and IT staff.

Answer: B

Explanation:

IT resource staffing requirements are the human resources needed to deliver IT services and support business objectives. Periodically evaluating IT resource staffing requirements is important to ensure the enterprise has sufficient resources to address changing business and IT needs, such as new projects, technologies, regulations, or customer expectations12. By assessing the current and future demand and supply of IT skills and competencies, the enterprise can identify any gaps or surpluses and plan accordingly to optimize IT performance and value34. The other options are not the primary reason for periodically evaluating IT resource staffing requirements, although they may be related or beneficial outcomes. Ascertaining the IT function has sufficient skilled staff to maintain daily operations, verifying that human resource recruitment and retention processes meet enterprise IT objectives, and confirming IT-related responsibilities are defined for the enterprise's business and IT staff are all part of the IT resource staffing management process, but they are not the main driver or purpose of it34. Reference:

3: https://www.aihr.com/blog/staffing-planning/

1: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our- insights/the-organization-blog/the-future-of-the-workplace-embracing-change-and-fostering- connectivity

2: https://www.ccl.org/articles/leading-effectively-articles/adaptability-1-idea-3-facts-5-tips/

4: https://www.indeed.com/career-advice/career-development/staffing-plan

Question: 265

Which of the following BEST indicates that a change management process has been implemented successfully?

A. Maturity levels
B. Degree of control
C. Process performance
D. Outcome measures

Answer: D

Explanation:

Outcome measures are tools used to assess the effect, both positive and negative, of an intervention or treatment1. Outcome measures can indicate whether a change management process has been implemented successfully by comparing the actual results of the change with the expected or desired results2. Outcome measures can also help evaluate the impact of the change on the organization's performance, quality, and value3. The other options are not the best indicators of successful change management implementation.

Maturity levels are a way of assessing the degree of development and sophistication of a process, but they do not necessarily reflect the outcomes or
benefits of the process4. Degree of control is a measure of how well aprocess is managed and monitored, but it does not capture the effectiveness or efficiency of the process. Process performance is a measure of how well a process meets its objectives and requirements, but it does not account for the outcomes or consequences of the process. Reference:

3: https://www.physio-pedia.com/Outcome_Measures
2: https://www.isc.hbs.edu/Documents/pdf/2020-outcome-measurement-feeley.pdf
1: https://en.wikipedia.org/wiki/Outcome_measure
4: https://www.coursera.org/articles/change-management-process
https://www.sciencedirect.com/topics/engineering/degree-of-control
https://www.sciencedirect.com/topics/engineering/process-performance

Question: 266

Following a re-prioritization of business objectives by management, which of the following should be performed FIRST to allocate resources to IT processes?

A. Perform a maturity assessment.
B. Implement a RACI model.
C. Refine the human resource management plan.
D. Update the IT strategy.

Answer: D

Explanation:

The IT strategy is the document that defines how IT will be used to support and achieve the business objectives of the organization. It aligns the IT investments, resources, and activities with the business priorities and direction. When there is a change in the business objectives, such as a re-prioritization by management, the IT strategy should be updated accordingly to ensure that IT remains relevant and aligned with the new business goals. Updating the IT strategy should be done first before allocating resources to IT processes, because it provides the basis for determining which IT processes are most critical and valuable for the organization. The other options are not the best actions to perform first in this scenario. Performing a maturity assessment, implementing a RACI model, and refining the human resource management plan are all useful activities for improving the IT processes, but they are not directly related to the change in business objectives. They should be done after updating the IT strategy, based on the new strategic direction and priorities. Reference: 1: https://www.projectpractical.com/human-resource-management-plan-template-free-download/ 2: https://open.lib.umn.edu/humanresourcemanagement/chapter/2-2-writing-the-hrm-plan/ 3: https://www.isixsigma.com/getting-started/are-you-ready-how-conduct-maturity-assessment/ 4: https://www.smartsheet.com/content/organizational-maturity
5: https://www.process.st/maturity-model/

Question: 267

IT security is concerned with employees' increasing use of personal equipment for work-related purposes, while employees claim it allows them to be more productive. A decision on whether to modify the enterprise information security policy should be based on:

A. audit findings.
B. user access approval procedures.
C. the impact to security.
D. a risk and benefit evaluation.

Answer: D

Explanation:

A risk and benefit evaluation is a method of weighing the pros and cons of an action or decision, such as modifying the enterprise information security policy to allow the use of personal equipment for work-related purposes. A risk and benefit evaluation can help identify the potential risks and benefits of such a change, assess their likelihood and impact, and compare them with the current situation or alternative options1. A risk and benefit evaluation can provide a systematic and objective basis for making a decision that balances the needs and interests of different stakeholders, such as IT security, employees, and the organization2. The other options are not the best basis for making a decision on whether to modify the enterprise information security policy. Audit findings are reports that evaluate the compliance and effectiveness of an existing policy or process, but they do not necessarily address the potential risks and benefits of changing it3. User access approval procedures are steps that authorize or deny users to access certain resources or systems, but they do not reflect the overall impact of using personal equipment for work-related purposes4. The impact to security is an important factor to consider, but it is not the only one. There may be other benefits or risks that need to be taken into account, such as productivity, cost, user satisfaction, etc.5 Reference: 5: https://www.osha.gov/personal-protective-equipment
4: https://www.ato.gov.au/Individuals/Income-deductions-offsets-and-records/Deductions-you-can-claim/Tools-computers-and-items-you-use-for-work/Tools-and-equipment-to-perform-your-work/ 3: https://www.ema.europa.eu/en/documents/presentation/presentation-periodic-safety-update- report-procedure-concept-benefit-risk-evaluation-r-postigo_en.pdf
2: https://safetyculture.com/topics/risk-analysis/
1: https://pestleanalysis.com/risk-benefit-analysis/

Question: 268

Which of the following is the PRIMARY consideration when developing an information asset management program?

A. Operational requirements
B. Industry best practice
C. Cost benefit
D. Regulatory requirements

Answer: D

Explanation:

Regulatory requirements are the rules and standards that an organization must follow to comply with the laws and regulations that apply to its industry, sector, or jurisdiction. Regulatory requirements can affect how an organization manages its information assets, such as data, documents, records, and reports. Information assets are valuable and sensitive resources that need to be protected from unauthorized access, use, disclosure, modification, or destruction1. Regulatory requirements can specify how information assets should be classified, labeled, handled, stored, transmitted, retained, disposed, and audited23. Failing to comply with regulatory requirements can result in legal penalties, reputational damage, financial losses, or operational disruptions for the organization3. Therefore, regulatory requirements are the primary consideration when developing an information asset management program. The other options are not the primary consideration when developing an
information asset management program, although they may be relevant or important factors. Operational requirements are the needs and expectations of the organization and its stakeholders for how information assets should support its business processes and

objectives4. Industry best practice are the methods and techniques that have proven to be effective and efficient in managing information assets in a similar context or domain5. Cost benefit is the analysis of the advantages and disadvantages of investing in an information asset management program in terms of resources, time, and money6. These options are all secondary or subordinate to regulatory requirements, because they do not have the same legal or mandatory force. An organization can choose to adapt or modify its operational requirements, industry best practice, or cost benefit analysis based on its situation and preferences, but it cannot ignore or violate its regulatory requirements without consequences. Reference:

1: https://www.cio.com/article/202183/what-is-data-governance-a-best-practices-framework-for- managing-data-assets.html

5: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/what-is-best-practice-in-information-security

4: https://www.gartner.com/en/information-technology/glossary/operational-requirements

2: https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to- iso-27001/

3: https://www.csoonline.com/article/570281/csos-ultimate-guide-to-security-and-privacy-laws-regulations-and-compliance.html

6: https://www.investopedia.com/terms/c/cost-benefitanalysis.asp

Question: 269

An enterprise is determining the objectives for an IT training improvement initiative from a governance prosected. it would be MOST important to ensure that:

A. policies and processes address both enterprise requirements and professional growth
B. courses of instruction that will maximize employee productivity are identified
C. several different training strategies are created for final approval by the CIO
D. IT employees are surveyed and interviewed to identify development needs

Answer: A

Explanation:

An enterprise is determining the objectives for an IT training improvement initiative from a governance perspective. Governance is the process of decision-making and implementation that involves various actors and structures, both formal and informal1. Governance aims to achieve good governance, which is characterized by participation, consensus, accountability, transparency, responsiveness, effectiveness, efficiency, equity, inclusion, and rule of law2. Therefore, it would be most important to ensure that the policies and processes for IT training address both the enterprise requirements and the professional growth of the IT employees. This would ensure that the IT training is aligned with the strategic goals and priorities of the enterprise, as well as the needs and expectations of the IT staff. It would also foster a culture of learning and development that enhances the performance, quality, and value of IT services345. The other options are not the most important objectives for an IT training improvement initiative from a governance perspective. Identifying courses of instruction that will maximize employee productivity, creating several different training strategies for final approval by the CIO, and surveying and interviewing IT employees to identify development needs are all useful steps or methods for designing and implementing an IT training improvement initiative, but they are not the ultimate objectives or outcomes. They are subordinate or instrumental to the main objective of addressing both the enterprise requirements and the professional growth of the IT employees through policies and processes that reflect good governance principles345. Reference:

3: https://topworkplaces.com/improving-training-and-development-strategies/

4: https://shrm.org/ResourcesAndTools/hr-topics/organizational-and-employee- development/Pages/Key-

Steps-for-Better-Training-Development-Programs.aspx

5: https://www.forbes.com/sites/forbeshumanresourcescouncil/2021/07/13/12-ways-to-implement-successful-employee-training-initiatives/

1: https://link.springer.com/article/10.1007/s40647-017-0197-4

2: https://www.unescap.org/sites/default/files/good-governance.pdf

Question: 270

Which of the following is the BEST way to maximize the value of an enterprise's information asset base?

A. Seek additional opportunities to leverage existing information assets.
B. Facilitate widespread user access to all information assets
C. Regularly purge information assets to minimize maintenance costs
D. Implement an automated information management platform

Answer: A

Explanation:

The value of an enterprise's information asset base is the amount of benefits or advantages that the enterprise can derive from its information assets, such as data, documents, records, and reports. Information assets are valuable and sensitive resources that need to be protected, managed, and used effectively and efficiently to support and achieve the enterprise's objectives and goals1. To maximize the value of an enterprise's information asset base, the best way is to seek additional opportunities to leverage existing information assets. This means finding new or innovative ways to use or reuse the information assets to create more value for the enterprise, such as improving performance, quality, customer satisfaction, innovation, or competitive advantage23. For example, an enterprise can leverage its existing information assets by analyzing them to generate insights, combining them to create new products or services, sharing them with partners or stakeholders to enhance collaboration, or monetizing them to generate revenue23.

The other options are not the best ways to maximize the value of an enterprise's information asset base. Facilitating widespread user access to all information assets may increase the availability and utilization of the information assets, but it may also compromise their confidentiality and integrity. Not all information assets are appropriate or relevant for all users, and some may contain sensitive or confidential data that need to be restricted or protected1 . Therefore, facilitating widespread user access to all information assets may not maximize their value, but rather increase their risk. Regularly purging information assets to minimize maintenance costs may reduce the storage and management expenses of the information assets, but it may also eliminate their potential value or usefulness. Not all information assets are obsolete or redundant, and some may have long-term or strategic value for the enterprise1 . Therefore, regularly purging information assets to minimize maintenance costs may not maximize their value, but rather decrease their availability. Implementing an automated information management platform may improve the efficiency and effectiveness of the information asset management process, but it may not necessarily increase the value of the information asset base. An automated information management platform is a tool or system that helps to collect, store, process, analyze, and distribute information
assets. However, it does not guarantee that the information assets are used or leveraged in optimal ways to create more value for the enterprise23. Therefore, implementing an automated information management platformmay not maximize the value of the information asset base, but rather facilitate its management.

Reference:

2: https://www.gartner.com/smarterwithgartner/why-and-how-to-value-your-information-as-an- asset

1: https://www.cio.com/article/202183/what-is-data-governance-a-best-practices-framework-for- managing-data-assets.html

3: https://www.gartner.com/en/publications/infonomics

https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso- 27001/
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk- assessment-and-control-implementation-model
https://www.ibm.com/topics/information-management-systems

Question: 271

The PRIMARY benefit of using an IT service catalog as part of the IT governance program is that it.

A. ensures IT effectively meets future business needs,
B. provides a foundation for measuring IT performance,
C. improves the ability to allocate IT resources
D. establishes enterprise performance metrics per service

Answer: B

Explanation:

An IT service catalog is a comprehensive list of all of the services an IT organization offers, such as IT support, IT operations, or IT projects. It usually includes a description of the service, its features, costs, and response and delivery times, as well as a method for requesting the service12. An IT service catalog is part of the IT governance program, which is a framework that provides a formal structure for aligning IT investments and activities with business objectives and ensuring IT effectiveness and efficiency34. The primary benefit of using an IT service catalog as part of the IT governance program is that it provides a foundation for measuring IT performance. By defining and documenting the IT services and their expected outcomes, an IT service catalog enables the IT organization to establish and monitor key performance indicators (KPIs) and service level agreements (SLAs) for each service. These metrics can help evaluate how well the IT services meet the customer needs and expectations, as well as the business goals and priorities. They can also help identify and address any gaps or issues in the IT service delivery and quality, and support continuous improvement and optimization125.

The other options are not the primary benefit of using an IT service catalog as part of the IT governance program, although they may be related or secondary benefits. Ensuring IT effectively meets future business needs, improving the ability to allocate IT resources, and establishingenterprise performance metrics per service are all desirable outcomes of using an IT service catalog, but they are not the main purpose or benefit. They are dependent or derived from the primary benefit of providing a foundation for measuring IT performance. By measuring IT performance, the IT organization can better understand the current and future business needs, allocate IT resources more efficiently and effectively, and align enterprise performance metrics with IT service outcomes125. Reference:

4: https://www.cio.com/article/272051/governanceit-governance-definition-and-solutions.html
2: https://www.atlassian.com/itsm/service-request-management/service-catalog
5: https://www.connectwise.com/blog/managed-services/it-service-catalog
1: https://www.servicenow.com/products/itsm/what-is-it-service-catalog.html
3: https://www.gartner.com/en/information-technology/glossary/it-governance

Question: 272

When developing an IT strategic plan that supports an enterprise's business goals which of the following should be done FIRST?

A. Ensure that IT drives business goals
B. Analyze benchmarking data
C. Understand the current vision
D. Perform a business impact analysis (BIA)

Answer: C

Explanation:

According to the ISACA CGEIT Exam Candidate Guide, one of the tasks under the domain of Strategic Alignment is to "understand the current vision and direction of the enterprise and identify how IT can best support it."1 This task should be done first when developing an IT strategic plan that supports an enterprise's business goals, because it provides the basis for aligning IT with the business strategy and priorities. By understanding the current vision and direction of the enterprise, the IT strategic plan can identify the gaps, opportunities, and challenges that need to be addressed by IT, as well as the expected outcomes and benefits that IT can deliver to the enterprise23. The other options are not the best actions to perform first in this scenario. Ensuring that IT drives business goals, analyzing benchmarking data, and performing a business impact analysis (BIA) are all useful steps or methods for developing an IT strategic plan, but they are not the starting point. They should be done after understanding the current vision and direction of the enterprise, based on the alignment and integration of IT with the business strategy and goals23. Reference:

1: https://www.isaca.org/-/media/info/cgeit/cgeit-exam-candidate-guide.pdf
2: https://www.cascade.app/blog/it-strategic-plan
3: https://www.projectmanager.com/blog/it-governance-frameworks-definitions

Question: 273

The PRIMARY reason for implementing an IT governance program in an enterprise is to

A. balance the demand for information and the ability to deliver.
B. complies with regulatory requirements
C. reduce risks due to improved compensating controls.
D. decrease the scale of investment in information systems due to budgetary controls.

Answer: A

Explanation:

IT governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives. IT governance helps align IT and business strategies, manage IT risks and benefits, and deliver value to key stakeholders. One of the main objectives of IT governance is to balance the demand for information and the ability to deliver it in an effective and efficient manner. Reference :=
CGEIT Review Manual 2023, Chapter 1: Framework for the Governance of Enterprise IT, page 8
CGEIT Review Questions, Answers & Explanations Manual 2023, Question 277, page 65

Question: 274

Which of the following is the BEST way to address an IT audit finding that many enterprise application updates lack appropriate documentation?

A. Enforce change control procedures.
B. Conduct software quality audits
C. Review the application development life cycle.
D. Add change control to the risk register.

Answer: A

Explanation:

Change control procedures are a set of steps that ensure that any changes to a system, product, project, or document are authorized, documented, and tracked. Change control procedures help to maintain the quality, integrity, and security of the system or product, as well as to comply with relevant standards and regulations.

By enforcing change control procedures, the enterprise can prevent unauthorized or undocumented updates that could compromise the functionality, performance, or reliability of the applications. Reference :=

What is a change control procedure? With benefits and steps

What is a change control process? Steps and template

Change Control | Risk Management & Audit Services - Harvard University

Question: 275

Which of the following is the GREATEST benefit of using a quantitative risk assessment method?

A. It uses resources more efficiently
B. It can be used to assess risks against non-tangible assets
C. It reduces subjectivity
D. It helps in prioritizing risk response action plans

Answer: C

Explanation:

A quantitative risk assessment method uses numerical values and mathematical models to estimate the likelihood and consequences of risks. This reduces the subjectivity and bias that may arise from qualitative methods that rely on personal judgment and experience. A quantitative method also allows for more objective comparison and prioritization of risks based on their impact and probability. Reference :=

Quantitative Risk Analysis (Definition, Benefits and Steps) - Indeed

Risk Assessment and Analysis Methods: Qualitative and Quantitative - ISACA

Question: 276

Following the rollout of an enterprise IT software solution that hosts sensitive data it was discovered that the application's role-based access control was not functioning as specified Which of the following is the BEST way to prevent reoccurrence in the future?

A. Ensure supplier contracts include penalties if solutions do not meet functional requirements
B. Ensure the evaluation process requires independent assessment of solutions prior to implementation
C. Ensure supplier contracts include a provision for the right to audit on an annual basis
D. Ensure procurement processes require the identification of alternate vendors to ensure business continuity.

Answer: B

Explanation:

An independent assessment is a review by a third party of an authorization decision, a product, a service, or a system to verify its quality, functionality, compliance, or performance. An independent assessment can help identify and mitigate potential risks, errors, or defects before they cause problems or failures. An independent assessment can also provide an objective and unbiased opinion on the suitability and effectiveness of a solution for a specific purpose or context.

By requiring an independent assessment of solutions prior to implementation, the enterprise can ensure that the solutions meet the functional requirements and specifications, as well as the security and privacy standards and policies. This can prevent issues such as the malfunctioning of role-based access control, which could compromise the confidentiality, integrity, and availability of sensitive data. An independent assessment can also help evaluate the compatibility and interoperability of solutions with existing systems and processes, and provide recommendations for improvement or optimization.

Some examples of independent assessment methods are:
Independent verification and validation (IV&V): A process that checks whether a system meets its defined requirements and specifications, and whether it fulfills its intended purpose and functions. Independent technical review (ITR): A process that evaluates the technical aspects of a system, such as its design, architecture, performance, reliability, security, usability, maintainability, and scalability. Independent security assessment (ISA): A process that assesses the security posture of a system, such as its vulnerability to threats, its compliance with security standards and regulations, its implementation of security controls and measures, and its response to security incidents.

Question: 277

An enterprise is considering outsourcing non-core IT processes Which of the following should be the FIRST step?

A. Update resource allocation policies
B. Conduct a cost-benefit analysis for outsourcing.
C. Issue a formal request for proposal to outsourcing vendors.
D. Establish service level metrics for outsourced activities

Answer: B

Explanation:

A cost-benefit analysis is a process that compares the costs and benefits of a decision or an action, such as outsourcing non-core IT processes. A cost-benefit analysis can help the enterprise evaluate the feasibility, profitability, and sustainability of outsourcing, as well as identify the potential risks and opportunities. A cost-benefit analysis can also help the enterprise determine the optimal level and scope of outsourcing, and select the most suitable outsourcing partner. A cost-benefit analysis should be the first step before issuing a formal request for proposal, establishing service level
metrics, or updating resource allocation policies. Reference :=
The Outsourcing Handbook A guide to outsourcing - Deloitte United Kingdom, page 10
Five Tips For Outsourcing Business Processes Effectively In 2021 - Forbes

Question: 278

The board of directors of an enterprise has questioned whether the business is focused on optimizing value.
The IT strategy committees' BEST action to address the board's concern is to:

A. initiate reporting and review of key IT performance metrics.
B. conduct a portfolio review to assess the benefits realization of IT investments.
C. conduct a benchmark to assess IT value relative to competitors.
D. form a technology council to monitor the efficiency of project implementation.

Answer: B

Explanation:

This is because a portfolio review is a process of evaluating the performance and value of IT investments in relation to the business objectives and strategy. A portfolio review can help to identify the alignment, contribution, and optimization of IT investments, as well as the risks, issues, and opportunities for improvement. A portfolio review can also help to communicate and demonstrate the value of IT to the board and other stakeholders, as well as to support decision-making and prioritization of IT resources.
Some of the sources that support this answer are:
1: This source explains the value of IT governance and how it can help to optimize risk and manage resources

to support the organization's mission, goals, and objectives. It also discusses some of the governance enablers, such as principles, processes, and policies, that can help to align IT with the business context.

2: This source provides a research-based methodology to improve IT governance and drive business results. It suggests that conducting a portfolio review is one of the steps to redesign the governance framework and ensure that IT investments are aligned with the business strategy and deliver value.

3: This source defines IT portfolio management as a discipline that enables organizations to manage their IT investments as a collection of projects, programs, and services that contribute to the enterprise's strategic goals. It also describes some of the benefits of IT portfolio management, such as improving alignment, optimizing value, reducing risk, and enhancing transparency.

Question: 279

Which of the following activities MUST be completed before developing an IT strategic plan?

A. Review the enterprise business plan
B. Align the enterprise vision statement with business processes
C. Develop an enterprise architecture (EA) framework
D. Review the enterprise risk tolerance level

Answer: A

Explanation:

Before developing an IT strategic plan, it is essential to review the enterprise business plan, which defines the enterprise's structure, governance, and operations. The enterprise business plan describes the enterprise's vision, mission, goals, objectives, strategies, and performance measures. It also outlines the enterprise's value proposition, market position, competitive advantage, and customer segments. The IT strategic plan should align with and support the enterprise business plan by providing a roadmap for how IT will enable and enhance the business capabilities and outcomes. The IT strategic plan should also consider the enterprise's risk appetite and tolerance, which are defined by the enterprise's risk management framework.

The other options are not necessarily required before developing an IT strategic plan. Aligning the enterprise vision statement with business processes is part of the IT strategic planning process, but it does not have to be done before developing the IT strategic plan. Developing an enterprise architecture (EA) framework is a separate activity that can be done in parallel or after developing the IT strategic plan. The EA framework defines how to create and use an enterprise architecture, which provides a holistic view of the organization's business, information, and technology. Reviewing the enterprise risk tolerance level is also part of the IT strategic planning process, but it does not have to be done before developing the IT strategic plan. The risk tolerance level reflects the acceptable level of variation around a particular set of risk-based objectives.

Question: 280

Which of the following is the BEST indication that information security requirements are taken into consideration when developing IT processes?

A. The database is deployed in a distributed processing platform
B. The information architecture incorporates data classification
C. Customer profiles are stored with a domestic service provider
D. The integrity of sensitive information is periodically reviewed

Answer: B

Explanation:

Data classification is a process of organizing and categorizing data based on its characteristics, confidentiality, and sensitivity. Data classification helps to determine the level of access and protection that data requires. Data classification also makes data easier to understand, compare, and analyze. Data classification is an essential part of information security, as it helps to align the security measures and policies with the data's value and risk. By incorporating data classification into the information architecture, the IT processes can ensure that information security requirements are taken into consideration from the design stage to the implementation stage. Reference := What is Data Classification? A Data Classification Definition
What is Sensitive Data? Definition, Examples, and More

Question: 281

To minimize the potential mishandling of customer personal information in a system located in a country with strict privacy regulations which of the following is the BEST action to take?

A. Update the information architecture
B. Revise the IT strategic plan
C. Implement data loss prevention (DLP)
D. Establish new IT key risk indicators (KRIs)

Answer: C

Explanation:
Data loss prevention (DLP) is a set of tools and processes that aim to prevent the unauthorized disclosure, misuse, or theft of sensitive data. DLP can help to minimize the potential mishandling of customer personal information in a system located in a country with strict privacy regulations by detecting and blocking any attempts to access, copy, or transfer the data without proper authorization or consent. Reference := CGEIT Review Manual, Chapter 4: Risk Optimization, Section 4.2: IT Risk Management Processes, Subsection 4.2.3: Risk Response, Page 155.

Question: 282

The IT department has determined that problems with a business report are due to quality issues within a set of data to whom should IT refer the matter for resolution?

A. Internal audit
B. Data architect
C. Business analyst
D. Data steward

Answer: D

Explanation:

A data steward is a subject matter expert who is responsible for defining and maintaining the integrity of a specific type of data or data domain1. They help the organization build data glossaries, create and maintain data quality rules, and determine who has access to data1. Data stewards also work closely with any system of record to ensure proper controls are in place and are maintained to ensure the data produced is of high quality2. Therefore, if the IT department has determined that problems with a business report are due to quality issues within a set of data, they should refer the matter to the data steward for resolution. Reference := CGEIT Review Manual, Chapter 3: Benefits Realization, Section 3.2: IT Value Delivery Processes, Subsection 3.2.4: Data Quality Management, Page 103.

Question: 283

Which of the following is the MOST important consideration when developing a new IT service'

A. Return on investment (ROI)
B. Resource requirements.
C. Service level agreements (SLAs)
D. Economies of scale

Answer: C

Explanation:

Service level agreements (SLAs) are the most important consideration when developing a new IT service, because they define the expectations and obligations of both the service provider and the service consumer. SLAs specify the scope, quality, availability, performance, and security of the IT service, as well as the roles and responsibilities, escalation procedures, and penalties for noncompliance. SLAs help to ensure that the IT service meets the business needs and objectives of the service consumer, and that the service provider delivers the IT service in a consistent and reliable manner. SLAs also provide a basis for measuring and improving the IT service delivery and management processes. Reference := CGEIT Review Manual, Chapter 3: Benefits Realization, Section 3.2: IT Value Delivery Processes, Subsection 3.2.1: IT Service Delivery, Page 93.

Question: 284

Which of the following BEST facilitates governance oversight of data protection measures?

A. Information ownership
B. Information classification
C. Information custodianship
D. Information life cycle management

Answer: A

Explanation:

Information ownership is the assignment of roles and responsibilities for data protection to individuals or groups within the organization. Information owners are accountable for ensuring that data is properly classified, secured, and used in accordance with the organization's policies and standards. Information ownership facilitates governance oversight of data protection measures by providing clear lines of authority and accountability for data assets. Reference:
ISACA CGEIT Review Manual 2021, page 86: "Information ownership is the assignment of roles and responsibilities for the protection of information to individuals or groups within the enterprise." ISACA CGEIT Review Questions, Answers & Explanations Manual 2021, page 11, question 14: "The correct answer is A. Information ownership is the assignment of roles and responsibilitiesfor the protection of information to individuals or groups within the enterprise. Information owners are accountable for ensuring that information is properly classified, secured, and used in accordance with the enterprise's policies and standards. Information ownership facilitates governance oversight of data protection measures by providing clear lines of authority and accountability for information assets."

Question: 285

An airline wants to launch a new program involving the use of artificial intelligence (AI) and machine learning the mam objective of the program is to use customer behavior to determine new routes and markets Which of the following should be done NEXT?

A. Consult with the enterprise privacy function
B. Define the critical success factors (CSFs)
C. Present the proposal to the IT strategy committee
D. Perform a business impact analysis (BIA)

Answer: B

Explanation:

Critical success factors (CSFs) are the essential elements or conditions that must be achieved for a project or program to be successful. CSFs help to define the scope, objectives, and expected outcomes of the project or program, as well as the key performance indicators (KPIs) and metrics to measure and evaluate the progress and results. CSFs also help to align the project or program with the strategic goals and vision of the organization, and to communicate the value proposition and benefits to the stakeholders. Therefore, before launching a new program involving the use of artificial intelligence (AI) and machine learning, an airline should define the CSFs to ensure that the program is feasible, desirable, and viable, and that it meets the business needs and expectations of the customers and the market. Reference := CGEIT Review Manual, Chapter 1: Framework for the Governance of Enterprise IT, Section 1.2: GEIT Principles, Subsection 1.2.3: Principle 3: Ensure Outcomes Are Delivered Through Effective Use of IT, Page 28.

Question: 286

Which of the following BEST facilitates the standardization of IT vendor selection?

A. Cost-benefit analysis
B. Contract management office
C. Service level agreements (SLAs)
D. Procurement framework

Answer: D

Explanation:

A procurement framework is a set of policies, procedures, and guidelines that govern the acquisition of goods and services from external sources. A procurement framework best facilitates the standardization of IT vendor selection, because it helps to ensure that the IT vendor selection process is consistent, transparent, fair, and efficient. A procurement framework also helps to define the roles and responsibilities, criteria and methods, documentation and reporting, and monitoring and evaluation of the IT vendor selection process. A procurement framework can help to reduce the risks, costs, and complexity of IT vendor selection, and to increase the quality, value, and performance of IT vendors. Reference := Software Selection, Page 2.

Question: 287

An IT governance committee is defining a risk management policy for a portfolio of IT-enabled investments Which of the following should be the PRIMARY consideration when developing the policy?

A. Risk management framework
B. Possible investment failures
C. Value obtained with minimum risk
D. Risk appetite of the enterprise

Answer: D

Explanation:

Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk appetite of the enterprise should be the primary consideration when developing a risk management policy for a portfolio of IT-enabled investments, because it helps to align the risk management strategy with the business strategy and goals. Risk appetite also helps to define the risk tolerance and thresholds for each investment, and to prioritize and allocate resources accordingly. Risk appetite also helps to communicate the

expectations and responsibilities of the stakeholders involved in the risk management process, and to foster a risk-aware culture within the organization. Reference := CGEIT Review Manual, Chapter 4: Risk Optimization, Section 4.1: IT Risk Management Strategy, Subsection 4.1.1: Establishing IT Risk Appetite, Page 139.

Question: 288

An internal audit revealed a widespread perception that the enterprise's IT governance reporting lacks transparency Which of the following should the CIO do FIRST?

A. Add stakeholder transparency metrics to the balanced scorecard
B. Develop a communication and awareness strategy
C. Meet with key stakeholders to understand their concerns
D. Adopt an industry-recognized template to standardize reports.

Answer: C

Explanation:

The CIO should first meet with key stakeholders to understand their concerns about the IT governance reporting transparency. This will help the CIO to identify the root causes of the perception, the expectations and needs of the stakeholders, and the gaps and issues in the current reporting process. Meeting with key stakeholders will also help to build trust and rapport, and to solicit feedback and suggestions for improvement. The CIO can then use this information to develop a communication and awareness strategy, adopt a standard template, and add transparency metrics to the balanced scorecard. These actions will help to enhance the transparency, consistency, and quality of the IT governance reporting, and to address the stakeholder concerns effectively. Reference := How Boards Realise IT Governance Transparency: A Study Into Current Practice of the COBIT EDM05 Process, Page 1.

Question: 289

An enterprise has decided to execute a risk self-assessment to identify improvement opportunities for current IT services. Which of the following is MOST important to address in the assessment?

A. Related business risk
B. Residual IT risk
C. Mapping of business objectives to IT risk
D. IT capability and performance measures

Answer: C

Explanation:

Mapping of business objectives to IT risk is the most important factor to address in a risk selfassessment for current IT services, because it helps to align the IT risk management strategy with the business strategy and goals. Mapping of business objectives to IT risk also helps to identify and prioritize the key IT risks that could affect the achievement of the business objectives, and to determine the appropriate risk responses and controls. Mapping of business objectives to IT risk also helps to communicate the value and benefits of IT risk management to the business stakeholders, and to foster a risk-aware culture within the organization. One of the sources that supports this answer is A Comprehensive Guide To Risk And Control Self -Assessment RCSA, which states that “RCSA aims to include the use of risk management techniques, business processes, and cultures in staff work and businesses to achieve objectives.”

Question: 290

Which of the following is MOST important for IT governance to have in place to ensure the enterprise can maintain operations during extensive system downtime?

A. Fault-tolerant hardware
B. An incident response plan
C. A crisis communications plan
D. A business continuity plan (BCP)

Answer: D

Explanation:

A business continuity plan (BCP) is the most important element for IT governance to have in place to ensure the enterprise can maintain operations during extensive system downtime. A BCP consists of the processes and procedures an organization needs to ensure its critical business processes continue operating during a disaster1. A BCP should include methods to ensure uninterrupted delivery of critical IT services, identify the resources needed, and outline manual workarounds. It should also contain policies, standards, procedures, and tools for responding to and preventing major incidents, as well as the IT architecture of the organization2. A BCP should be reviewed regularly and updated as needed.
Reference := Business continuity planning (BCP) - Learning Center, IT Business Continuity | DisasterRecovery.org, IT Governance Blog: free business continuity plan template

Question: 291

Which of the following is MOST important for an enterprise to review when classifying information assets?
A. Procedures for information handling
B. Requirements for information retention.
C. Media used for storage and backup
D. Impact of information exposure

Answer: D

Explanation:

The impact of information exposure is the most important factor for an enterprise to review when classifying information assets, because it helps to determine the level of sensitivity and protection that the information assets require. Information assets are classified according to their confidentiality, integrity, and availability, which reflect the potential harm or loss that could result from unauthorized disclosure, modification, or destruction of the information assets. The impact of information exposure can be assessed in terms of financial, reputational, legal, operational, or strategic consequences for the enterprise and its stakeholders. The impact of information exposure can also vary depending on the context, scope, and duration of the exposure. Therefore, by reviewing the impact of information exposure, an enterprise can assign appropriate labels and controls to its information assets, and ensure that they are handled and stored securely and appropriately.
Reference := Information classification according to ISO27001, Information Asset and Security Classification Procedure, Information Classification Standard.

Question: 292

Which of the following is MOST important to document for a business ethics program?
A. Guiding principles and best practices
B. Violation response matrix
C. Whistle-blower protection protocols.
D. Employee awareness and training content

Answer: A

Explanation:

Guiding principles and best practices are the most important elements to document for a business ethics program, because they provide the foundation and direction for the program. Guiding principles are the core values and beliefs that inform the ethical behavior and decision-making of the organization and its stakeholders. Best practices are the methods and techniques that have been proven to be effective and efficient in achieving the desired ethical outcomes. Documenting guiding principles and best practices helps to communicate the purpose, scope, and objectives of the business ethics program, as well as the roles and responsibilities, policies and procedures, standards and expectations, and evaluation and improvement mechanisms. Documenting guiding principles and best practices also helps to align the business ethics program with the organizational strategy and culture, and to foster a consistent and coherent ethical environment.

Reference := How to Build a Business Ethics Program - Bizmanualz, A Guide for Business How to develop a Human rights Policy.

Question: 293

Which of the following is the BEST outcome measure to determine the effectiveness of IT nsk management processes?

A. Frequency of updates to the IT risk register
B. Time lag between when IT risk is identified and the enterprise's response
C. Number of events impacting business processes due to delays in responding to risks
D. Percentage of business users satisfied with the quality of risk training

Answer: C

Explanation:

The number of events impacting business processes due to delays in responding to risks is the best outcome measure to determine the effectiveness of IT risk management processes, because it reflects the actual consequences and losses that result from inadequate or ineffective riskmanagement. Outcome measures are metrics that evaluate the results and benefits of a process or activity, rather than the inputs or outputs1. Outcome measures help to assess whether the process or activity is achieving its objectives and delivering value to the organization1. The number of events impacting business processes due to delays in responding to risks is an outcome measure that indicates how well the IT risk management processes are able to identify, analyze, evaluate, treat, monitor, and communicate IT risks in a timely and appropriate manner. A high number of such events would suggest that the IT risk management processes are not effective, and that they need to be improved or revised. A low number of such events would suggest that the IT risk management processes are effective, and that they are reducing the likelihood and impact of IT risks on the organization.

Reference := How To Measure Risk Management KPI & Metrics - ERM Software

Question: 294

An IT department outsourced application support and negotiated service level agreements (SLAs) directly with the vendor Although the vendor met the SLAs business owner expectations are not met and senior management cancels the contract This situation can be avoided in the future by:

A. improving the business requirements gathering process
B. improving the negotiation process for service level agreements (SLAs)
C. implementing a vendor performance scorecard
D. assigning responsibility for vendor management

Answer: D

Explanation:

Assigning responsibility for vendor management is the best way to avoid the situation where the IT department outsourced application support and negotiated service level agreements (SLAs) directly with the vendor, but the business owner expectations were not met and senior management cancelled the contract. Vendor management is the process of managing the relationship with a supplier, also known as a vendor or a third party1. Vendor management involves selecting, contracting, monitoring, evaluating, and communicating with vendors to ensure that they deliver the goods and services that meet the business needs and objectives1. Assigning responsibility for vendor management helps to ensure that there is a clear and consistent governance structure, strategy, and policy for working with vendors2. It also helps to align the expectations and interests of all the stakeholders involved, such as the IT department, the business owners, and the senior management2. Assigning responsibility for vendor management also helps to avoid duplication of efforts, conflicts of interest, or gaps in oversight that could result in poor vendor performance, dissatisfaction, or risk exposure2.

Reference := 9 vendor management best practices for 2023 - Juro, Best Practices for Vendor Management | Smartsheet.

Question: 295

An IT value delivery framework PRIMARILY helps an enterprise

A. increase transparency of value to the enterprise
B. assist top management in approving IT projects
C. improve value of successful IT projects
D. optimize value to the enterprise.

Answer: D

Explanation:

An IT value delivery framework primarily helps an enterprise optimize value to the enterprise, because it provides a systematic and holistic approach to planning, building, and delivering IT solutions that meet the business needs and objectives. An IT value delivery framework helps to align IT strategy with business strategy, ensure effective governance and management of IT resources and processes, measure and monitor IT performance and outcomes, and continuously improve IT value creation and delivery1. An IT value delivery framework also helps to balance the benefits, costs, and risks of IT investments, and to ensure that IT delivers value to the enterprise in terms of efficiency, effectiveness, agility, innovation, and customer satisfaction2.

Reference := IT Governance: Definition, Frameworks, and Best Practices - InvGate, What is ValueBased Delivery? | Blog | Digital.ai.

Question: 296

Which of the following IT governance practices would BEST support IT and enterprise strategic alignment?

A. An IT communication plan is continuously updated
B. External consultants regularly review the IT portfolio
C. Senior management regularly reviews the IT portfolio
D. IT service level agreements (SLAs) are periodically updated

Answer: C

Explanation:

Senior management regularly reviewing the IT portfolio is the best IT governance practice to support IT and enterprise strategic alignment, because it helps to ensure that the IT investments are aligned with the business strategy and goals, and that they deliver value to the enterprise. An IT portfolio is a collection of IT projects,

programs, services, and assets that support the business objectives and processes of an organization1. Senior management regularly reviewing the IT portfolio helps to prioritize, monitor, and evaluate the IT investments based on their performance, benefits, costs, and risks2. It also helps to identify and address any gaps, issues, oropportunities for improvement in the IT portfolio2. Senior management regularly reviewing the IT portfolio also helps to communicate and collaborate with the IT department and other stakeholders, and to provide guidance and direction for the IT strategy and governance2.

Reference := IT Portfolio Management: A Simplified Guide | Planview, IT Governance – How to align IT and business strategy?

Question: 297

Which of the following is the BEST way for an organization to minimize the difference between expected and delivered services when acquiring resources?

A. Negotiate service level agreements (SLAs)
B. Measure service delivery using industry benchmarks
C. Require quarterly benefits realization reporting
D. Include a right-to-audit clause in the contract.

Answer: A

Explanation:

Negotiating service level agreements (SLAs) is the best way for an organization to minimize the difference between expected and delivered services when acquiring resources, because SLAs define the scope, quality, availability, performance, and security of the services that the provider will deliver to the customer. SLAs also specify the roles and responsibilities, escalation procedures, and penalties for non-compliance of both parties. By negotiating SLAs, the organization can ensure that its expectations and requirements are clearly communicated and agreed upon by the provider, and that there are mechanisms to measure and monitor the service delivery and outcomes. Negotiating SLAs also helps to prevent or resolve any disputes or issues that may arise from the service provision, and to ensure that the organization receives the value and benefits that it expects from the provider. One of the sources that supports this answer is Service-level Agreement: 3 Types And Templates - Contract Lawyers, which states that “A service-level agreement is important because it: Protects both parties: The SLA sets standards for the service, ensuring both the service provider and end user are on the same page with expectations.”

Question: 298

Which of the following is (he GREATEST benefit of using the life cycle approach to govern information assets?

A. Overall costs are optimized
B. Operational costs are maintained
C. Information availability is improved
D. Compliance with regulatory requirements is ensured

Answer: A

Explanation:

Using the life cycle approach to govern information assets is the greatest benefit for an organization, because it helps to optimize the overall costs associated with the creation, storage, processing, distribution, and disposition of information. The life cycle approach involves managing information according to its value, utility, and risk throughout its lifespan1. By using the life cycle approach, an organization can ensure that it only collects, creates, and retains the information that is relevant, accurate, and useful for its business objectives

and processes2. It can also ensure that it stores, protects, and disposes of the information in a cost-effective and secure manner, complying with the legal and regulatory requirements2. The life cycle approach also helps to improve the performance, availability, and accessibility of the information, as well as its quality and integrity3. By using the life cycle approach, an organization can reduce the operational costs, storage costs, compliance costs, and risk exposure costs associated with its information assets4. Therefore, using the life cycle approach to govern information assets is the greatest benefit for an organization.
Reference := What is Information Lifecycle Management (ILM)?, Information Lifecycle Management: A Comprehensive Guide, Information Lifecycle Management (ILM) - Gartner IT Glossary, The Comprehensive Guide to Information Lifecycle Management.

Question: 299

Which of the following provides the BEST information to assess the effective alignment of IT investments?

A. IT balanced scorecard
B. Net present value (NPV).
C. IT delivery time metrics
D. Total cost of ownership (TCO)

Answer: A

Explanation:

An IT balanced scorecard is the best information source to assess the effective alignment of IT investments, because it provides a comprehensive and balanced view of the IT performance and value from four perspectives: financial, customer, internal process, and learning and growth1. An IT balanced scorecard helps to translate the IT strategy and objectives into measurable indicators that reflect the contribution of IT to the business strategy and goals2. An IT balanced scorecard also helps to monitor and evaluate the IT investments based on their benefits, costs, and risks, and to identify and address any gaps or issues in the IT alignment2. An IT balanced scorecard also helps to communicate and report the IT value and outcomes to the stakeholders, and to foster a continuous improvement culture within the organization2.
Reference := Implementing the IT Balanced Scorecard: Aligning IT with … - Routledge, Strategy-Based Balanced Scorecards for Technology.

Question: 300

An enterprise is planning a transformation initiative by leveraging emerging technology that will have a significant impact on existing products and services Which of the following is the BEST way for IT to prepare for this change?

A. Use a balanced scorecard to measure IT outcomes.
B. Analyze emerging technology products and related training needs.
C. Procure appropriate resources to support emerging technology
D. Assess the impact on the existing IT strategy

Answer: D

Explanation:

The best way for IT to prepare for a transformation initiative by leveraging emerging technology that will have a significant impact on existing products and services is to assess the impact on the existing IT strategy. An IT strategy is a plan that defines how IT will support the business strategy and objectives, and how IT will deliver value to the enterprise1. By assessing the impact of the emerging technology on the existing IT strategy, IT can determine whether the current IT vision, mission, goals, and capabilities are aligned with the transformation

initiative, and whether they need to be revised or updated2. Assessing the impact of the emerging technology on the existing IT strategy also helps IT to identify and prioritize the opportunities, challenges, and risks that the emerging technology may bring, and to develop appropriate solutions and responses3. Assessing the impact of the emerging technology on the existing IT strategy also helps IT to communicate and collaborate with the business stakeholders, and to ensure that the IT investments are aligned with the business needs and expectations4.

Reference := IT Strategy: What is it?, How to create an effective IT strategy in 2022, Emerging Technology Strategy: A Guide for CIOs, Maximizing Emerging Technology Adoption Benefits - Gartner

Question: 301

Which of the following would be MOST helpful to an enterprise that wants to standardize how sensitive corporate data is handled?

A. Information classification framework
B. Enterprise risk policy
C. Enterprise risk management (ERM) framework
D. Information security policy

Answer: A

Explanation:

An information classification framework would be the most helpful to an enterprise that wants to standardize how sensitive corporate data is handled, because it provides a systematic and consistent way to identify, label, and protect the data according to its level of sensitivity and the impact of its exposure. An information classification framework helps to define the criteria and methods for classifying data into different categories, such as public, internal, confidential, or secret1. It also helps to specify the roles and responsibilities, policies and procedures, standards and expectations, and tools and techniques for handling data securely and appropriately throughout its life cycle2. An information classification framework also helps to comply with the legal and regulatory requirements, and to reduce the risks, costs, and complexity associated with data management3. Reference := Information classification – How to do it according to ISO 27001, Create a well-designed data classification framework, Information classification framework diagram.

Question: 302

When selecting a vendor to provide services associated with a critical application which of the following is the MOST important consideration with respect to business continuity planning (BCP)? A. Procuring a copy of the vendor's BCP during the contracting process

B. Testing the vendor's BCP and analyzing the results
C. Obtaining independent audit reports of the vendor's BCP
D. Evaluating whether the vendor's BCP aligns with the enterprise's BCP

Answer: D

Explanation:

Evaluating whether the vendor’s BCP aligns with the enterprise’s BCP is the most important consideration when selecting a vendor to provide services associated with a critical application, because it helps to ensure that the vendor can meet the service level agreements (SLAs) and recovery objectives of the enterprise in the event of a disruption or disaster. A BCP is a plan that defines how an organization will continue its critical business processes and functions during and after a crisis1. A vendor’s BCP should be

compatible and consistent with the enterprise's BCP, and should address the specific risks, impacts, and requirements of the service provision2. Evaluating whether the vendor's BCP aligns with the enterprise's BCP helps to avoid any gaps, conflicts, or issues that could affect the availability, performance, and quality of the service, and to ensure that the vendor can restore the service within an acceptable time frame3. Evaluating whether the vendor's BCP aligns with the enterprise's BCP also helps to comply with the regulatory and contractual obligations, and to protect the reputation and value of the enterprise4.
Reference := Business Continuity Planning (BCP) Definition, Business Continuity Planning for Vendors: What You Need to Know, Vendor Business Continuity Plan: How to Ensure Your Vendors Are Prepared for Disasters, Business Continuity Planning for Vendors: 5 Steps to Success.

Question: 303

IT management has reported difficulty retaining qualified IT personnel to support the organization's new strategy Given that outsourcing is not a viable approach, which of the following would be the BEST way for IT governance to address this situation?

A. Implement an incentive-based employee referral program
B. Direct the development of a strategic HR plan for IT
C. Recommend enhancements to the online recruiting platform specific to IT
D. Work with HR to enhance compensation packages for IT personnel

Answer: B

Explanation:

A strategic HR plan is a document that drives the business forward by evaluating where the workforce is at and comparing it to future needs. It sets out the organizational goals and outlines how the HR team will help achieve them1. A strategic HR plan for IT would help to identify and address the gaps, challenges, and opportunities in the IT talent management, such as recruitment, retention, development, engagement, and succession2. A strategic HR plan for IT would also help to align the IT workforce with the IT strategy and objectives, and to ensure that the IT personnel have the skills, competencies, and motivation to support the organization's new strategy3. A strategic HR plan for IT would also help to communicate and collaborate with the IT personnel and other stakeholders, and to foster a positive and supportive IT culture4.

Question: 304

Which of the following is the BEST approach to assist an enterprise in planning for iT-enabled investments?

A. Enterprise architecture (EA).
B. IT process mapping
C. Task management
D. Service level management

Answer: A

Explanation:

The best approach to assist an enterprise in planning for IT-enabled investments is enterprise architecture (EA). EA is a holistic and integrated view of the current and future state of the business, IT, and their alignment1. EA helps to identify and prioritize the business needs andobjectives, and to design and deliver the IT solutions that support them2. EA also helps to optimize the IT resources and processes, and to ensure that they are aligned with the business strategy and goals3. EA also helps to measure and monitor the IT performance and outcomes, and to evaluate the value and benefits of the IT investments4. EA also helps to manage the risks,

costs, and complexity of the IT investments, and to ensure that they comply with the legal and regulatory requirements5.

IT process mapping, task management, and service level management are not as comprehensive or effective as EA in assisting an enterprise in planning for IT-enabled investments. IT process mapping is a visual representation of a process that shows the steps and their relationships6. It can help to understand how a process works, but it does not provide a strategic or architectural view of the business or IT. Task management is a process of managing individual or group tasks to achieve goals7. It can help to track and delegate work, but it does not address the alignment or optimization of IT with the business. Service level management is a process of defining, documenting, and agreeing on service levels within an IT service management system8. It can help to ensure that services are delivered at an agreed level, but it does not cover the design or delivery of IT solutions that meet the business needs. Therefore, EA is the best approach to assist an enterprise in planning for IT-enabled investments.

Question: 305

Before establishing IT key nsk indicators (KRIs) which of the following should be defined FIRST?

A. IT resource strategy
B. IT risk and security framework
C. IT goals and objectives
D. IT key performance indicators (KPIs)

Answer: C

Explanation:

IT goals and objectives are the desired outcomes and targets that IT aims to achieve in support of the business strategy and objectives. IT goals and objectives should be defined first before establishing IT key risk indicators (KRIs), because they provide the direction and scope for the IT risk management process. KRIs are metrics that measure and monitor the level and trend of risk exposure, and help to identify and manage potential threats or opportunities that could affect the achievement of IT goals and objectives1. Therefore, by defining IT goals and objectives first, an enterprise can ensure that its KRIs are relevant, aligned, and consistent with its IT strategy and value delivery2. Reference := Key Risk Indicators (KRIs) - ISACA, Integrating KRIs and KPIs for Effective Technology Risk Management - ISACA.

Question: 306

Which of the following should be the ClO's GREATEST consideration when making changes to the IT strategy'?

A. Has the impact to the enterprise architecture (EA) been assessed?
B. Has the investment portfolio been revised?
C. Have key stakeholders been consulted?
D. Have IT risk metrics been adjusted?

Answer: C

Explanation:

The CIO’s greatest consideration when making changes to the IT strategy should be whether key stakeholders have been consulted, because they are the ones who are affected by and involved in the IT strategy. Key stakeholders include the business functions, customers, suppliers, partners, regulators, and employees who depend on or contribute to the IT value delivery1. Consulting key stakeholders helps to ensure that the IT strategy is aligned with the business strategy and objectives, and that it meets the needs and expectations of the stakeholders2. Consulting key stakeholders also helps to solicit feedback and suggestions for improvement, and to gain buy-in and support for the IT strategy3. Consulting key stakeholders also helps to identify and manage any risks, issues, or opportunities that may arise from the IT strategy changes4.

Reference := IT Strategy: What is it?, How to create an effective IT strategy in 2022, IT Strategy Stakeholder Engagement, IT Strategy: A 3-step Plan.

Question: 307

An independent consultant has been hired to conduct an ad hoc audit of an enterprise's information security office with results reported to the IT governance committee and the board Which of the following is MOST important to provide to the consultant before the audit begins?

A. Acceptance of the audit risks and opportunities
B. The scope and stakeholders of the audit
C. The organizational structure of the security office
D. The policies and framework used by the security office

Answer: B

Explanation:

The scope and stakeholders of the audit are the most important information to provide to the consultant before the audit begins, because they define the objectives, boundaries, and expectations of the audit. The scope and stakeholders of the audit are also part of the IT governance domain 1: Framework for the Governance of Enterprise IT1. Reference := 1: CGEIT Review Manual 2023, ISACA, page 23.

Question: 308

Which of the following should be the MOST important consideration when designing an implementation plan for IT governance?

A. Principles and policies
B. Roles and responsibilities
C. Risk tolerance levels
D. Organizational culture

Answer: D

Explanation:

Organizational culture is the most important consideration when designing an implementation plan for IT governance, because it influences the ethics, values, behaviors, and attitudes of the people involved in the governance process. Organizational culture also affects the acceptance, adoption, and sustainability of the IT governance framework and practices. According to COBIT 5, one of the seven enablers of IT governance is culture, ethics and behavior1. The roadmap for implementing and improving IT governance also emphasizes the importance of understanding and addressing the cultural and behavioral aspects of the enterprise2. Reference := 1: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, page 312: A Roadmap for Implementing and Improving IT Governance1

Question: 309

Enterprise leadership is concerned with the potential for discrimination against certain demographic groups resulting from the use of machine learning models What should be done FIRST to address this concern?

A. Obtain stakeholders' input regarding the ethics associated with machine learning
B. Revise the code of conduct to discourage bias within automated processes
C. Develop a machine learning policy articulating guidelines for machine learning use
D. Assess recent case law related to the enterprise's machine learning business strategy

Answer: A

Explanation:

The first step to address the concern of discrimination against certain demographic groups resulting from the use of machine learning models is to obtain stakeholders' input regarding the ethics associated with machine learning. This is because stakeholders are the ones who are affected by or have an interest in the outcomes of machine learning models, and their input can help identify the ethical values, principles, and standards that should guide the development and use of machine learning models. Stakeholders' input can also help ensure that the machine learning models are aligned with the enterprise's mission, vision, and goals, as well as the legal and regulatory requirements. According to COBIT 5, one of the seven enablers of IT governance is stakeholders1. The Ethics and Governance of Artificial Intelligence project also emphasizes the importance of engaging with diverse stakeholders to ensure that AI systems are fair,accountable, transparent, and human-centric2. Reference := 1: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, page 312: Algorithms and Justice - Berkman Klein Center

Question: 310

An enterprise has identified a number of plausible risk scenarios that could result in economic loss associated with major IT investments. Which of the following is the BEST method to assess the risk?

A. Cost-benefit analysis
B. Qualitative analysis
C. Business impact analysis (BIA)
D. Quantitative analysis

Answer: D

Explanation:

Quantitative analysis is the best method to assess the risk of plausible scenarios that could result in economic loss associated with major IT investments, because it tries to assign objective numerical or measurable values to the components of the risk assessment and to the assessment of potential loss1. Quantitative analysis can help estimate the probability and impact of risk events, calculate the expected monetary value (EMV) of risk, and compare the costs and benefits of different risk responses2. Quantitative analysis can also provide a more accurate and objective basis for decision making than qualitative analysis, which is scenario-based and relies on subjective judgments1. Reference := 1: Risk Assessment and Analysis Methods: Qualitative and Quantitative - ISACA12: 6 Types of Risk Assessment Methodologies + How to Choose - Drata2

Question: 311

Which of the following should be the PRIMARY basis for establishing categories within an information classification scheme?

A. Information architecture
B. Industry standards
C. Information security policy
D. Business impact

Answer: D

Explanation:

The primary basis for establishing categories within an information classification scheme should be the

business impact, because it reflects the level of importance and sensitivity of the information to the organisation and its stakeholders. The business impact can be assessed by considering the potential consequences of unauthorised disclosure, modification, or loss of availability of the information. The higher the business impact, the higher the level of protection required for the information. For example, information that could cause severe damage to the organisation's reputation, operations, or finances if compromised should be classified as Top Secret1, whereas information that is intended for public release should be classified as Public2. The information security policy should provide guidance on how to classify information based on the business impact, but it is not the primary basis for establishing categories. The information architecture and industry

standards may also influence the classification scheme, but they are not as relevant as the business impact.

Question: 312

An enterprise will be adopting wearable technology to improve business performance Whtch of the following would be the BEST way for the CIO to validate IPs preparedness for this initiative?

A. Request an enterprise architecture (EA) review.
B. Request reprioritization of the IT portfolio.
C. Perform a baseline business value assessment
D. Identify the penalties for noncompliance.

Answer: A

Explanation:

The best way for the CIO to validate IT's preparedness for adopting wearable technology to improve business performance is to request an enterprise architecture (EA) review. An EAreview is a comprehensive analysis of the current and future state of the enterprise's IT architecture, including its alignment with the business strategy, goals, and objectives. An EA review can help identify the gaps, risks, opportunities, and requirements for implementing wearable technology in the enterprise, as well as evaluate the feasibility, costs, benefits, and impacts of the initiative. An EA review can also provide recommendations and guidance for the design, development, integration, and governance of wearable technology solutions within the enterprise's IT environment. According to COBIT 5, one of the seven enablers of IT governance is enterprise architecture1. The EA review is also part of the IT governance domain 2: Strategic Alignment2. Reference := 1: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, page 312: CGEIT Review Manual 2023, ISACA, page 69.

Question: 313

Which of the following is a responsibility of an IT strategy committee?

A. Providing oversight on enterprise strategy implementation
B. Approving the business strategy and its IT implications
C. Advising the board on the development of IT goals
D. Tracking projects in the IT investment portfolio

Answer: C

Explanation:

One of the responsibilities of an IT strategy committee is to advise the board on the development of IT goals that are aligned with the enterprise strategy and objectives. The IT strategy committee is a high-level governance body that provides guidance and direction on IT matters to the board and management. The IT strategy committee does not approve the business strategy or its IT implications, as this is the role of the

board. The IT strategy committee also does not provide oversight on enterprise strategy implementation or track projects in the IT investment portfolio, as these are the roles of the management and the IT steering committee, respectively123. Reference := 1: PART 2 – CISA Domain 2 – Governance and Management of IT12: TO STEER OR TO STRATEGIZE –DIFFERENCES BETWEEN IT STEERING COMMITTEES AND IT STRATEGY COMMITTEES43: Building an IT Governance Committee - HBS Working Knowledge

Question: 314

When establishing a risk management process which of the following should be the FIRST step?

A. Determine the probability of occurrence
B. Identify threats
C. Identify assets
D. Assess risk exposures

Answer: C

Explanation:

The first step in establishing a risk management process is to identify assets, because assets are the resources that have value to the organization and need to be protected from potential threats. Assets can include physical, human, information, financial, and intangible assets. Identifying assets helps to determine their criticality, ownership, and dependencies, as well as the potential impact of losing or compromising them. According to the ISO 31000:2018 standard, one of the components of the risk management framework is establishing the context, which includes defining the scope, objectives, and criteria for risk management, as well as identifying the internal and external factors that can affect the achievement of objectives1. Identifying assets is part of establishing the context. The other steps of the risk management process, such as identifying threats, determining the probability of occurrence, assessing risk exposures, and implementing risk treatments, follow after identifying assets. Reference := 1: ISO 31000:2018(en), Risk management — Guidelines

Question: 315

Which of the following would be the BEST long-term solution to address the concern regarding loss of experienced staff?

A. implement knowledge management practices
B. Establish a mentoring program for IT staff
C. Determine key risk indicators (KRIs)
D. Retain key staff as consultants.

Answer: A

Explanation:

The best long-term solution to address the concern regarding loss of experienced staff is to implement knowledge management practices, because knowledge management is the process of creating, sharing, using, and managing the knowledge and information of an organization1. Knowledge management practices can help capture, document, and transfer the valuable knowledge and expertise of the experienced staff before they leave the organization, as well as facilitate the learning and development of the new or existing staff. Knowledge management practices can also enhance the organizational performance, innovation, and competitiveness by leveraging the intellectual capital and creating a culture of knowledge sharing2. According to a study by 3, the impact of knowledge management practices on employee retention is significant and positive in both IT and banking industries. Another study by 4 found that knowledge management practices can improve job satisfaction and employee retention by fostering a supportive work environment, providing growth opportunities, and rewarding knowledge contributions. Therefore, implementing knowledge

management practices can help mitigate the risk of losing experienced staff and their knowledge in the long run.

The other options are not the best long-term solutions, because they are either short-term or partial solutions. Establishing a mentoring program for IT staff can help transfer some of the knowledge and skills of the experienced staff to the mentees, but it may not be sufficient or systematic enough to capture and preserve all the relevant knowledge. Determining key risk indicators (KRIs) can help monitor and measure the risk exposure of losing experienced staff, but it does not address the root cause or provide a solution for the problem. Retaining key staff as consultants can help retain some of the expertise and experience of the staff, but it may not be feasible or cost-effective in the long term, and it may also create dependency and vulnerability issues for the organization.

Question: 316

An enterprise has performed a business impact analysis (BIA) considering a number of risk scenarios Which of the following should the enterprise do NEXT?

A. Perform a risk controls gap analysis
B. Update the disaster recovery plan (DRP)
C. Verify compliance with relevant legislation
D. Assess risk mitigation strategies

Answer: D

Explanation:

The next step that the enterprise should do after performing a business impact analysis (BIA) considering a number of risk scenarios is to assess risk mitigation strategies. A risk mitigation strategy is a plan of action that aims to reduce the likelihood or impact of a risk event, or to transfer or accept the risk1. Assessing risk mitigation strategies involves evaluating the costs, benefits, feasibility, and effectiveness of various options for addressing the risks identified in the
BIA. Assessing risk mitigation strategies can help the enterprise prioritize and implement the most appropriate and efficient solutions for protecting its critical business processes and resources from potential disruptions2. According to the Business Continuity Planning Process Diagram, assessing risk mitigation strategies is the fourth step in the business continuity planning process, following the BIA3.

The other options are not the next steps that the enterprise should do after performing a BIA. Performing a risk controls gap analysis is a step that precedes the BIA, as it helps to identify the existing controls and their effectiveness in preventing or reducing the risks4. Updating the disaster recovery plan (DRP) is a step that follows after assessing risk mitigation strategies, as it involves documenting the procedures and resources for restoring the critical business functions and IT systems in case of a disaster5. Verifying compliance with relevant legislation is a step that is done throughout the business continuity planning process, as it ensures that the enterprise meets the legal and regulatory requirements for its industry and location6. Reference := 1: Risk Mitigation Strategies - ISACA72: How to Conduct aComprehensive Business Impact Analysis: A Step-by-Step Guide33: Business Continuity Planning Process Diagram - ISACA84: Business Impact Analysis: Definition and How To Conduct One15: The Complete Guide to Business Impact Analysis with Templates - Creately46: How To Conduct Business Impact Analysis in 8 Easy Steps - G25

Question: 317

An enterprise has finalized a major acquisition and a new business strategy in line with stakeholder needs has been introduced to help ensure continuous alignment of IT with the new business strategy
the CiO should FIRST

A. review the existing IT strategy against the new business strategy
B. revise the existing IT strategy to align with the new business strategy

C. establish a new IT strategy committee for the new enterprise
D. assess the IT cultural aspects of the acquired entity

Answer: A

Explanation:

The first step that the CIO should do to help ensure continuous alignment of IT with the new business strategy is to review the existing IT strategy against the new business strategy. A review is a process of evaluating and comparing the current state and performance of the IT strategy with the desired state and expectations of the new business strategy. A review can help identify the strengths, weaknesses, opportunities, and threats of the IT strategy, as well as the gaps, risks, and issues that need to be addressed. A review can also provide insights and recommendations for improving and aligning the IT strategy with the new business strategy. According to COBIT 5, one of the seven enablers of IT governance is performance management, which includes reviewing and monitoring the achievement of IT-related goals and objectives1. The review is also part of the IT governance domain 2: Strategic Alignment2.

The other options are not the first steps that the CIO should do to ensure continuous alignment of IT with the new business strategy. Revising the existing IT strategy to align with the new business strategy is a step that follows after reviewing the existing IT strategy, as it involves making changes and adjustments to the IT strategy based on the findings and recommendations of the review. Establishing a new IT strategy committee for the new enterprise is a step that may or may not be necessary depending on the existing governance structure and processes, and it does not directly address the alignment issue. Assessing the IT cultural aspects of the acquired entity is a step that may be relevant for integrating and harmonizing the IT functions and practices of both entities, but it does not ensure alignment with the new business strategy. Reference := 1: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, page 312: CGEIT Review Manual 2023, ISACA, page 69.

Question: 318

An enterprise has decided to implement an IT risk management program After establishing stakeholder desired outcomes, the MAIN goal of the IT strategy committee should be to: A. identify business data that requires protection.

B. perform a risk analysis on key IT processes
C. implement controls to address high risk areas
D. ensure IT risk alignment with enterprise risk

Answer: D

Explanation:

The main goal of the IT strategy committee after establishing stakeholder desired outcomes should be to ensure IT risk alignment with enterprise risk. IT risk alignment means that the IT risk management program is consistent and integrated with the enterprise risk management (ERM) program, and that the IT risks are identified, assessed, and treated in relation to the enterprise's objectives, strategies, and risk appetite. IT risk alignment can help the enterprise achieve the following benefits1:

Enhance the value delivery of IT to the business
Improve the decision making and prioritization of IT investments and initiatives
Reduce the likelihood and impact of IT-related incidents and losses
Increase the resilience and agility of IT in responding to changes and disruptions Strengthen the governance and accountability of IT performance and compliance To ensure IT risk alignment with enterprise risk, the IT strategy committee should perform the following tasks2:

Define the scope, objectives, and criteria for IT risk management

Establish the roles and responsibilities for IT risk management

Align the IT risk management framework and processes with the ERM framework and processes Communicate and collaborate with the ERM function and other stakeholders on IT risk issues Monitor and review the effectiveness and maturity of IT risk management

The other options are not the main goal of the IT strategy committee after establishing stakeholder desired outcomes. Identifying business data that requires protection, performing a risk analysis on key IT processes, and implementing controls to address high risk areas are steps that are part of the IT risk management process, but they are not specific to ensuring IT risk alignment with enterprise risk. These steps should be done by the IT risk management function or team, under the guidance and oversight of the IT strategy committee.

Question: 319

An enterprise has learned of a new regulation that may impact delivery of one of its core technology services

Which of the following should the done FIRST?

A. Update the risk management framework
B. Determine whether the board wants to comply with the regulation
C. Assess the risk associated with the new regulation
D. Request an action plan from the risk team

Answer: C

Explanation:

The first thing that the enterprise should do after learning of a new regulation that may impact delivery of one of its core technology services is to assess the risk associated with the new regulation. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and impacts of a risk event on the enterprise's objectives, processes, and resources1. A risk assessment can help the enterprise understand the nature, scope, and severity of the new regulation, as well as its compliance requirements, costs, and benefits. A risk assessment can also help the enterprise prioritize and implement the appropriate risk responses, such as avoiding, reducing, transferring, or accepting the risk2. According to COBIT 5, one of the seven enablers of IT governance is risk management, which includes assessing IT-related risks and aligning them with enterprise risks3. The risk assessment is also part of the IT governance domain 3: Risk Management4.

The other options are not the first things that the enterprise should do after learning of a new regulation. Updating the risk management framework is a step that may be done after assessing the risk associated with the new regulation, as it involves reviewing and improving the policies, procedures, and practices for managing IT risks in the enterprise. Determining whether the board wants to comply with the regulation is a step that may be done after assessing the risk associated with the new regulation, as it involves consulting with the board and other stakeholders on the

strategic and ethical implications of complying or not complying with the regulation. Requesting an action plan from the risk team is a step that may be done after assessing the risk associated with the new regulation, as it involves defining and executing the tasks and activities for achieving compliance and mitigating risk.

Question: 320

The BEST way for a CIO to monitor the alignment between the business and IT strategy is to regularly review

A. key risk indicators (KRIs)
B. IT services supporting business processes
C. the balanced scorecard
D. the risk register

Answer: C

Explanation:

The best way for a CIO to monitor the alignment between the business and IT strategy is to regularly review the balanced scorecard. The balanced scorecard is a strategic management tool that helps to measure and communicate the performance of an organization in relation to its vision, mission, goals, and objectives. The balanced scorecard uses four perspectives: financial, customer, internal process, and learning and growth, to evaluate how well the organization is achieving its desired outcomes and creating value for its stakeholders1. The balanced scorecard can also help to align the IT strategy with the business strategy by linking the IT objectives, initiatives, and measures with the business objectives, initiatives, and measures across the four perspectives2. By reviewing the balanced scorecard regularly, the CIO can monitor the progress and results of the IT strategy, identify the gaps and issues that need to be addressed, and ensure that the IT strategy is supporting and enabling the business strategy. According to COBIT 5, one of the seven enablers of IT governance is performance management, which includes using the balanced scorecard to align IT-related goals and metrics with enterprise goals and metrics3. The balanced scorecard is also part of the IT governance domain 5: Performance Measurement4.

The other options are not the best ways for a CIO to monitor the alignment between the business and IT strategy. Key risk indicators (KRIs) are metrics that indicate the level of risk exposure or potential impact of a risk event on an organization. KRIs can help to monitor and manage IT risks, but they do not necessarily reflect the alignment of IT strategy with business strategy. IT services supporting business processes are the activities and functions that IT provides to enable and facilitate the execution of business processes. Reviewing IT services can help to evaluate the quality and efficiency of IT delivery, but they do not capture the strategic alignment of IT with business. The risk register is a document that records and tracks the identified risks, their causes, impacts, probabilities, responses, owners, and statuses. The risk register can help to document and communicate IT risks, but it does not measure or report the alignment of IT strategy with business strategy.

Reference := 1: Balanced Scorecard Basics - Balanced Scorecard Institute12: Aligning Business Strategy with Information Technology Strategy - ISACA23: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, page 314: CGEIT Review Manual 2023, ISACA, page 197. : Key Risk Indicators - ISACA3 : What are IT Services? Definition & Examples - BMC Software4 : Risk Register - ISACA

Question: 321

The FIRST step in aligning resource management to the enterprise's IT strategic plan would be to

A. develop a responsible, accountable, consulted and informed (RACI) chart
B. assign appropriate roles and responsibilities
C. perform a gap analysis
D. identify outsourcing opportunities

Answer: C

Explanation:

The first step in aligning resource management to the enterprise's IT strategic plan would be to perform a gap analysis. A gap analysis is a process of comparing the current state and performance of the IT resources with the desired state and expectations of the IT strategic plan. IT resources include people, processes, technology, and information that support the delivery and management of IT services and solutions1. A gap analysis can help identify the strengths, weaknesses, opportunities, and threats of the IT resources, as well as the gaps, risks, and issues that need to be addressed. A gap analysis can also provide insights and recommendations for improving and aligning the IT resources with the IT strategic plan. According to 2, one of the steps in developing an IT strategic plan is to conduct a gap analysis to assess the current capabilities and

resources of the IT organization and determine the gaps between the current and future states.
The other options are not the first steps in aligning resource management to the enterprise's IT strategic plan. Developing a responsible, accountable, consulted and informed (RACI) chart is a step that may be done after performing a gap analysis, as it involves defining and clarifying the roles and responsibilities of the IT stakeholders for each task or activity in the IT strategic plan3. Assigning appropriate roles and responsibilities is a step that may be done after performing a gap analysis, as it involves allocating and delegating the IT resources to the relevant tasks or activities in the IT strategic plan. Identifying outsourcing opportunities is a step that may be done after performing a gap analysis, as it involves evaluating and selecting external vendors or partners that can provide IT services or solutions that are not available or feasible internally4. Reference := 1: What are IT Resources? Definition & Examples - BMC Software13: RACI Chart: Definition & Example - Project Management34: Outsourcing: Definition & Examples - Investopedia42: How to Create an Effective IT Strategy - Smartsheet2

Question: 322

Which of the following should a new CIO do FIRST to ensure information assets are effectively governed?

A. Quantify the business value of information assets
B. Perform an information gap analysis
C. Review information classification procedures
D. Evaluate information access methods

Answer: B

Explanation:

The first thing that a new CIO should do to ensure information assets are effectively governed is to perform an information gap analysis. An information gap analysis is a process of comparing the current state and performance of the information assets with the desired state and expectations of the information governance program. Information assets include data, metadata, documents, and
records that have value to the organization and need to be managed andprotected. An information gap analysis can help identify the strengths, weaknesses, opportunities, and threats of the information assets, as well as the gaps, risks, and issues that need to be addressed. An information gap analysis can also provide insights and recommendations for improving and aligning the information assets with the information governance program. According to 1, an information gap analysis is a key step in developing an information governance strategy that supports the organization's goals and objectives.
The other options are not the first things that a new CIO should do to ensure information assets are effectively governed. Quantifying the business value of information assets is a step that may be done after performing an information gap analysis, as it involves measuring and communicating the benefits and costs of the information assets to the organization and its stakeholders. Reviewing information classification procedures is a step that may be done after performing an information gap analysis, as it involves evaluating and updating the policies and practices for categorizing and labeling the information assets according to their sensitivity and criticality. Evaluating information access methods is a step that may be done after performing an information gap analysis, as it involves assessing and improving the mechanisms and controls for granting and restricting access to the information assets.

Question: 323

An IT steering committee wants to select a disaster recovery site based on available risk data Which of the following would BE ST enable the mapping of cost to risk?

A. Key risk indicators (KRIs)
B. Scenario-based assessment
C. Business impact analysis (BIA)

D. Qualitative forecasting

Answer: C

Explanation:

The best way to enable the mapping of cost to risk for selecting a disaster recovery site based on available risk data is to perform a business impact analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of various disaster scenarios on the critical business functions and processes of an organization. A BIA can help estimate the financial and operational impacts of losing or disrupting the business functions and processes, such as revenue loss, customer dissatisfaction, regulatory fines, contractual penalties, reputation damage, etc. A BIA can also help determine the recovery time objectives (RTOs) and recovery point objectives (RPOs) for each business function and process, which indicate how quickly and how much data they need to be restored after a disaster. By performing a BIA, the IT steering committee can map the cost of each disaster recovery site option to the risk of each disaster scenario, and compare the trade-offs between different levels of protection and investment1.

The other options are not the best ways to enable the mapping of cost to risk for selecting a disaster recovery site. Key risk indicators (KRIs) are metrics that indicate the level of risk exposure or potential impact of a risk event on an organization. KRIs can help monitor and manage IT risks, but they do not necessarily reflect the cost of different disaster recovery site options. Scenario-based assessment is a method of analyzing and evaluating the likelihood and consequences of various risk scenarios. Scenario-based assessment can help identify and prioritize IT risks, but it does not provide a clear measure of the cost of different disaster recovery site options. Qualitative forecasting is a technique of using expert opinions, judgments, or intuition to predict future outcomes or trends.

Qualitative forecasting can help estimate the future demand or growth of IT services, but it does not provide a reliable or objective basis for mapping the cost to risk of different disaster recovery site options.

Question: 324

An enterprise incurred penalties for noncompliance with privacy regulations. Which of the following is MOST important to ensure appropriate ownership of access controls to address this deficiency?

A. Granting access to information based on information architecture
B. Engaging an audit of logical access controls and related security policies
C. Implementing multi-factor authentication controls
D. Authenticating access to information assets based on roles or business rules

Answer: A

Explanation:

The most important thing to ensure appropriate ownership of access controls to address the deficiency of noncompliance with privacy regulations is to grant access to information based on information architecture. Information architecture is the design and organization of information and data in a way that supports the business objectives, processes, and requirements. Information architecture can help define the ownership, classification, and protection of information assets, as well as the roles, responsibilities, and rules for accessing and managing them. By granting access to information based on information architecture, the enterprise can ensure that only authorized and legitimate users can access the information that they need, and that the information is handled in accordance with the privacy regulations and policies. According to 1, access control is an essential element of security that determines who is allowed to access certain data, apps, and resources—and in what circumstances. According to 2, a privacy management framework provides steps to meet the ongoing compliance obligations under privacy principles, such as establishing robust and effective privacy

practices, procedures and systems.

The other options are not the most important things to ensure appropriate ownership of access controls to address the deficiency of noncompliance with privacy regulations. Engaging an audit of logical access controls and related security policies is a step that may be done after grantingaccess to information based on information architecture, as it involves verifying and testing the effectiveness and compliance of the access controls and policies. Implementing multi-factor authentication controls is a step that may be done after granting access to information based on information architecture, as it involves enhancing the security and verification of the user identity and credentials. Authenticating access to information assets based on roles or business rules is a step that may be done after granting access to information based on information architecture, as it involves implementing a specific type of access control mechanism that assigns permissions and restrictions based on predefined roles or business rules.

Question: 325

Which of the following would BEST support an enterprise's initiative to incorporate desired organizational behaviors into the IT governance framework?

A. Enterprise code of ethics
B. Risk mitigation strategies and action plans
C. Documented consequences for noncompliance
D. Enterprise RACI matrix

Answer: A

Explanation:

An enterprise code of ethics is a set of principles and values that guide the behavior and decisionmaking of the organization and its members. It can help to incorporate desired organizational behaviors into the IT governance framework by establishing a common understanding and expectation of what is acceptable and unacceptable, and by promoting a culture of integrity, accountability, and responsibility. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 17.

Question: 326

To develop appropriate measures to improve organizational performance, the measures MUST be:

A. a result of benchmarking and comparative analysis.
B. accepted by and meaningful to the stakeholders.
C. based on existing and validated data sources.
D. approved by the IT steering committee.

Answer: B

Explanation:

To develop appropriate measures to improve organizational performance, the measures must be accepted by and meaningful to the stakeholders, because they are the ones who will use the measures to monitor and evaluate the achievement of the enterprise’s objectives and goals. Themeasures should be relevant, reliable, valid, and understandable for the stakeholders, and aligned with their expectations and needs . Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 43-44.

Question: 327

When considering an IT change that would enable a potential new line of business, the FIRST strategic step for IT governance would be to ensure agreement among the stakeholders regarding: A. objectives to achieve goals.

B. metrics to measure effectiveness
C. a vision for the future state,

D. a change response plan

Answer: C

Explanation:

When considering an IT change that would enable a potential new line of business, the first strategic step for IT governance would be to ensure agreement among the stakeholders regarding a vision for the future state, because this would provide a clear direction and purpose for the change, and align the IT strategy with the business strategy. A vision statement should describe the desired outcomes and benefits of the change, and reflect the enterprise's mission, values, and goals12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 23-24.

Question: 328

Which of the following should be the PRIMARY consideration for an enterprise when prioritizing IT projects?

A. Technical capability of the enterprise to execute the projects
B. Process owner expectations based on operational benefits
C. Results of IT performance benchmarks against competitors
D. Impact on the business due to expected project outcomes

Answer: D

Explanation:

When prioritizing IT projects, the primary consideration for an enterprise should be the impact on the business due to expected project outcomes, because this would align the IT investments with the enterprise's strategic objectives and value creation. The impact on the business can be assessed by using criteria such as return on investment (ROI), net present value (NPV), risk exposure, customer satisfaction, and competitive advantage12. Reference:= ISACA, CGEIT Review Manual, 7th Edition, 2019, page 31-32.

Question: 329

An enterprise is planning to migrate its IT infrastructure to a cloud-based solution but does not have experience with this technology Which of the following should be done FIRST to reduce the risk of IT service disruptions when using this new technology?

A. Implement key performance indicators (KPIs).
B. Reflect the change in the enterprise architecture (EA).
C. Evaluate the sourcing options.
D. Engage an experienced IT consultant to perform the migration.

Answer: D

Explanation:

An enterprise that is planning to migrate its IT infrastructure to a cloud-based solution but does not have experience with this technology should first engage an experienced IT consultant to perform the migration, because this would reduce the risk of IT service disruptions when using this new technology. An experienced IT consultant can help the enterprise to assess the feasibility, benefits, and risks of the cloud migration, design and implement a suitable cloud architecture, and ensure a smooth transition and integration of the existing and new IT systems. An experienced IT consultant can also provide guidance and training to the enterprise's IT staff on how to manage and operate the cloud-based solution effectively and securely12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 65-66.

Question: 330

Which of the following roles should be responsible for data normalization when it is found that a new system includes duplicates of data items?

A. Business system owner
B. Data steward
C. Database administrator (DBA)
D. Application manager

Answer: B

Explanation:

A data steward is a role that is responsible for data normalization when it is found that a new system includes duplicates of data items, because a data steward is accountable for the quality, integrity, and consistency of the data in the enterprise. A data steward can define and enforce data standards, policies, and rules, and perform data cleansing, validation, and reconciliation activities to ensure that the data is accurate, complete, and reliable12.

Question: 331

As part of the implementation of IT governance, the board of an enterprise should establish an IT strategy committee to:

A. provide input to and ensure alignment of the enterprise and IT strategies.
B. ensure IT risks inherent in the enterprise strategy implementation are managed
C. drive IT strategy development and take responsibility for implementing the IT strategy.
D. assume governance accountability for the business strategy on behalf of the board

Answer: A

Explanation:

As part of the implementation of IT governance, the board of an enterprise should establish an IT strategy committee to provide input to and ensure alignment of the enterprise and IT strategies, because this would enable the board to oversee and direct the IT function in a way that supports the enterprise's vision, mission, goals, and objectives. The IT strategy committee should consist of board members and senior executives who have a stake in the IT performance and value delivery, and who can communicate and coordinate with other board committees and business units. The IT strategy committee should also review and approve the IT strategic plan, monitor the IT performance and outcomes, and ensure the alignment of IT resources and capabilities with the enterprise's needs and expectations1 . Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 19-20.

Question: 332

An enterprise has identified potential environmental disasters that could occur in the area where its data center is located. Which of the following should be done NEXT?

A. Implement an early warning detection and notification system.
B. Assess the likelihood and impact on the data center.
C. Relocate the data center to minimize the threat.
D. Assess how the data center is protected against the threat.

Answer: B

Explanation:

An enterprise that has identified potential environmental disasters that could occur in the area where its data center is located should next assess the likelihood and impact on the data center, because this would help to evaluate the level of risk and prioritize the appropriate risk response strategies. The likelihood and impact assessment should consider the frequency, severity, duration,
and scope of the potential disasters, and the potential consequences for the data center's availability, integrity, confidentiality, and performance12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 75-76.

Question: 333

Which of the following should IT governance mandate before any transition of data from a legacy system to a new technology platform?

A. Data conversion has documented approvals from business process data owners.
B. Data conversion is performed in a test environment to confirm correctness
C. Control totals of key transaction values are matched with data converted for migration.
D. A crisis management plan has been approved by the IT steering committee

Answer: A

Explanation:

Data conversion is the process of transforming data from one format or system to another. It is a critical activity in any data migration or integration project, as it affects the quality, accuracy, and usability of the data. Therefore, IT governance should mandate that data conversion has documented approvals from business process data owners, who are the stakeholders responsible for defining and maintaining the data requirements, standards, and quality for their respective business processes. This ensures that the data conversion meets the business needs and expectations, as well as complies with the relevant policies and regulations. Reference:

CGEIT Review Manual 2021, Chapter 4: Resource Optimization, Section 4.2: Data Management, page 1651
CGEIT Review Questions, Answers & Explanations Manual 2021, Question 10, page 252
Data Conversion: Definition, Best Practices, and Examples3
Data Governance Roles and Responsibilities4

Question: 334

A CIO of an enterprise is concerned that IT and the business have different priorities. Which of the following would BEST demonstrate the current state of strategic alignment?

A. IT maturity model
B. Business case
C. Balanced scorecard
D. IT investment status

Answer: C

Explanation:

A balanced scorecard is a tool that would best demonstrate the current state of strategic alignment, because it is a framework that translates the enterprise's vision and strategy into a set of performance measures that

cover four perspectives: financial, customer, internal business process, and learning and growth12. A balanced scorecard can help to assess how well the IT function is supporting the business objectives, and identify the gaps and opportunities for improvement. A balanced scorecard can also help to communicate and monitor the IT strategy and goals, and align the IT activities and resources with the business needs and expectations1 .

Question: 335

Which of the following would a CIO use to present the overall view of IT performance to the board of directors?

A. Balanced scorecard
B. Key risk indicators (KRIs)
C. Maturity model
D. Key performance indicators (KPIs)

Answer: A

Explanation:

A balanced scorecard is a tool that a CIO would use to present the overall view of IT performance to the board of directors, because it is a framework that translates the enterprise's vision and strategy into a set of performance measures that cover four perspectives: financial, customer, internal business process, and learning and growth12. A balanced scorecard can help to communicate and monitor the IT strategy and goals, and align the IT activities and resources with the business needs and expectations. A balanced scorecard can also provide a balanced and comprehensive view of the IT performance and value delivery, and highlight the strengths, weaknesses, opportunities, and threats for improvement12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 4344.

Question: 336

Which of the following is the BEST justification for a procurement manager to agree to purchase IT equipment from a specific vendor during a sales promotion?

A. The IT benefit surpasses the business benefit from the purchase.
B. The equipment adds value to the enterprise.
C. The business profit surpasses the IT cost for the equipment.
D. The product is offered at the lowest price.

Answer: B

Explanation:

A procurement manager should agree to purchase IT equipment from a specific vendor during a sales promotion only if the equipment adds value to the enterprise. This means that the equipment supports the business goals and objectives, meets the current and future needs of the stakeholders, and delivers benefits that outweigh the costs and risks. The procurement manager should also consider the quality, reliability, compatibility, and security of the equipment, as well as the vendor's reputation, service level, and warranty.

The other options are not the best justification for a procurement manager to agree to purchase IT equipment from a specific vendor during a sales promotion. The IT benefit surpasses the business benefit from the purchase is not a valid justification, as it implies that the IT department's interests are more important than the enterprise's interests. The procurement manager should align the IT strategy with the business strategy and ensure that the IT equipmentsupports the enterprise value creation. The business profit surpasses the IT cost for the equipment is not a sufficient justification, as it does not account for other factors such as quality,

Watermark Sample

performance, functionality, and risk of the equipment. The procurement manager should evaluate the total cost of ownership (TCO) and return on investment (ROI) of the IT equipment, not just the initial purchase price. The product is offered at
the lowest price is not a convincing justification, as it does not guarantee that the equipment is suitable for the enterprise's needs and expectations. The procurement manager should not compromise on quality, functionality, or security for a lower price.

For more information on IT procurement and value creation, you can refer to these web sources: IT Procurement Manager Job Description w/ Role & Responsibilities

IT Governance: Definitions, Frameworks and Planning

What is Governance in Procurement? Its Model

What is IT governance? A formal way to align IT & business strategy

Question: 337

When evaluating the process for acquiring third-party IT resources, management identified several suppliers with repeated downtime issues impacting the enterprise. Which of the following is the BEST approach to help ensure future service delivery in accordance with business objectives?

A. Establish key performance indicators (KPIs)
B. Appoint a procurement oversight committee
C. Establish key risk indicators (KRIs).
D. Implement contract monitoring.

Answer: D

Explanation:

The best approach to help ensure future service delivery in accordance with business objectives is to implement contract monitoring, because this would enable the enterprise to measure and evaluate the performance and compliance of the third-party IT suppliers, and identify and resolve any issues or gaps that may affect the service quality, availability, and reliability. Contract monitoring should involve defining and tracking key performance indicators (KPIs), key risk indicators (KRIs), service level agreements (SLAs), and contractual obligations, and applying corrective actions or penalties when necessary12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 67-68.

Question: 338

Which of the following should be the PRIMARY input when developing IT strategy?

A. Vision statement
B. Process and capability maturity
C. Governance objectives
D. Balanced scorecard

Answer: A

Explanation:

A vision statement should be the primary input when developing IT strategy, because it is a concise and clear expression of the enterprise's desired future state and direction, and it reflects the enterprise's mission, values, and goals12. A vision statement can help to guide and inspire the IT function to align its activities and resources with the business needs and expectations, and to deliver value and innovation to the enterprise. A vision statement can also help to communicate and monitor the IT strategy and objectives, and measure the IT performance and outcomes12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page

23-24.

Question: 339

Due to the recent introduction of personal data protection regulations, an enterprise is required to maintain its employee data in production systems only for a limited time. Which of the following is MOST important to review?

A. Asset retention policies
B. Information retention policies
C. Data archival policies
D. Data backup and restoration policies

Answer: B

Explanation:

Information retention policies are the most important to review, because they define the rules and procedures for retaining, disposing, and destroying information in accordance with the legal, regulatory, and business requirements. Information retention policies can help the enterprise to comply with the personal data protection regulations, and to ensure the privacy, security, and availability of the employee data in production systems12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 57-58.

Question: 340

A data governance strategy has been defined by the IT strategy committee which includes privacy objectives related to access controls, authorized use. and data collection. Which of the following should the committee do NEXT?

A. Mandate data privacy training for employees.
B. Establish a data privacy budget
C. Perform a data privacy impact assessment.
D. Mandate the creation of a data privacy policy.

Answer: D

Explanation:

The IT strategy committee should mandate the creation of a data privacy policy next, because this would provide a formal and consistent framework for implementing and enforcing the data governance strategy and the privacy objectives related to access controls, authorized use, and data collection. A data privacy policy should define the roles and responsibilities of the data owners, stewards, custodians, and users, and specify the principles, standards, and procedures for collecting, processing, storing, sharing, and disposing of personal data in compliance with the legal and regulatory requirements12. A data privacy policy should also include the mechanisms for monitoring and auditing the data privacy practices, and for handling any data breaches or incidents12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 57-58.

Question: 341

Which of the following is the MOST appropriate mechanism for measuring overall IT organizational performance?

A. IT portfolio return on investment (ROI)
B. Maturity model
C. IT balanced scorecard
D. Service level metrics

Answer: C

Explanation:

An IT balanced scorecard is the most appropriate mechanism for measuring overall IT organizational performance, because it is a framework that translates the enterprise's vision and strategy into a set of performance measures that cover four perspectives: financial, customer, internal business process, and learning and growth12. An IT balanced scorecard can help to communicate and monitor the IT strategy and goals, and align the IT activities and resources with the business needs and expectations. An IT balanced scorecard can also provide a balanced and comprehensive view of the IT performance and value delivery, and highlight the strengths, weaknesses, opportunities, and threats for improvement12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 4344.

Question: 342

A large enterprise has decided to use an emerging technology that needs to be integrated with the current IT infrastructure. Which of the following is the BEST way to prevent adverse effects to the enterprise resulting from the new technology?

A. Develop key performance indicators (KPIs).
B. Update the risk appetite statement
C. Develop key risk indicators (KRIs).
D. Implement service level agreements (SLAs)

Answer: C

Explanation:

The best way to prevent adverse effects to the enterprise resulting from the new technology is to develop key risk indicators (KRIs), because they are metrics that measure the potential impact and likelihood of the risks associated with the new technology, and provide early warning signals for taking corrective actions. KRIs can help the enterprise to monitor and manage the risks of integrating the new technology with the current IT infrastructure, and to ensure that the expected benefits and value are realized12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 75-76.

Question: 343

Which of the following would be the BEST way for an IT steering committee to monitor the adoption of a new enterprise IT strategy?

A. Establish key performance indicators (KPIs).
B. Establish key risk indicators (KRIs).
C. Schedule ongoing audit reviews.
D. Implement service level agreements (SLAs)

Answer: A

Explanation:

The best way for an IT steering committee to monitor the adoption of a new enterprise IT strategy is to establish key performance indicators (KPIs), because they are metrics that measure the progress and achievement of the IT strategic objectives and goals, and provide feedback and guidance for improvement. KPIs can help the IT steering committee to track and evaluate the performance and outcomes of the IT function, and to ensure that the IT activities and resources are aligned with the business needs and expectations12. KPIs can also help to communicate and report the IT value delivery and innovation to the board

and other stakeholders12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 43-44.

Question: 344

Which of the following is the MOST important input for the development of a human resources strategy to address IT skill gaps?

A. Training budget allocated for IT staff
B. Training effectiveness reports
C. Technology direction of the enterprise
D. A recent IT skills matrix

Answer: C

Explanation:

The most important input for the development of a human resources strategy to address IT skill gaps is the technology direction of the enterprise, because this would help to identify the current and future IT capabilities and competencies that are required to support the enterprise's vision, mission, goals, and objectives. The technology direction of the enterprise should consider the external and internal factors that influence the IT environment, such as market trends, customer demands, innovation opportunities, regulatory requirements, and business strategies12. The human resources strategy should align the IT staff development and retention plans with the technology direction of the enterprise, and ensure that the IT staff have the relevant skills, knowledge, and experience to deliver value and performance to the enterprise12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 25-26.

Question: 345

An enterprise wishes to establish key risk indicators (KRIs) in an effort to better manage IT risk.
Which of the following should be identified FIRST?

A. Risk mitigation strategies
B. Enterprise architecture (EA) components
C. The enterprise risk appetite
D. Key performance metrics

Answer: C

Explanation:

An enterprise that wishes to establish key risk indicators (KRIs) in an effort to better manage IT risk should first identify the enterprise risk appetite, because this would help to define the level of risk that the enterprise is willing and able to accept in pursuit of its objectives and value creation. The enterprise risk appetite should consider the external and internal factors that influence the IT environment, such as market trends, customer demands, innovation opportunities, regulatory requirements, and business strategies12. The KRIs should align with the enterprise risk appetite, and measure the potential impact and likelihood of the risks that may affect the IT performance and
outcomes12. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 75-76.

Question: 346

Which of the following would be the BEST way to facilitate the successful adoption of a new technology across the enterprise?

A. Ensure the use of a business case
B. Review business goals.
C. Establish an IT balanced scorecard.

D. Highlight the risk the new technology will address.

Answer: A

Explanation:

The best way to facilitate the successful adoption of a new technology across the enterprise is to ensure the use of a business case, because this would help to justify the need, benefits, and value of the new technology, and to gain the support and commitment of the stakeholders. A business case should include the objectives, scope, requirements, costs, risks, and expected outcomes of the new technology, and how it aligns with the enterprise's vision, mission, goals, and strategy12. A business case should also provide a clear roadmap and plan for implementing and managing the new technology, and for measuring and evaluating its performance and impact12.

Question: 347

Which of the following should be the FIRST consideration for an enterprise faced with a pandemic situation resulting in a mandatory remote work environment?

A. Reviewing and testing disaster recovery plans (DRPs)
B. Ensuring staff has the necessary technology to be productive
C. Ensuring remote work policies are updated and communicated
D. Revising IT performance monitoring metrics

Answer: B

Explanation:

The first consideration for an enterprise faced with a pandemic situation resulting in a mandatory remote work environment should be ensuring staff has the necessary technology to be productive, because this would enable the enterprise to maintain its business continuity and resilience, and to minimize the disruption and loss of the IT services and capabilities. The necessary technology may include hardware, software, network, security, and communication tools that support the remote work activities and requirements of the staff12. The enterprise should also provide guidance and training to the staff on how to use the technology effectively and securely12. The other options are not the first consideration, because they are either dependent on or secondary to the availability and functionality of the technology.

Question: 348

The MAIN responsibility of the board of directors regarding the management of enterprise risk is to:

A. ensure a risk process exists which addresses the risk appetite.
B. sustain investment in staff training regarding IT risk.
C. promote a benefits-driven culture throughout the enterprise.
D. maintain awareness of IT risk to the business.

Answer: A

Explanation:

The main responsibility of the board of directors regarding the management of enterprise risk is to ensure a risk process exists which addresses the risk appetite, because this would help the board to oversee and direct the enterprise's risk management activities and ensure that they are aligned with the enterprise's strategic objectives and value creation. The risk process should include identifying, assessing, responding, monitoring, and reporting the risks that may affect the enterprise's performance and outcomes, and ensuring that the risks are within the acceptable level that the enterprise is willing and able to tolerate12. The other options are not

the main responsibility of the board of directors, because they are either part of or dependent on the risk process.

Question: 349

Which of the following BEST supports an enterprise's ability to comply with privacy laws and regulations?

A. Complete inventory of enterprise data
B. Implementation of a breach notification process
C. Accurate classification of enterprise data
D. Robust enterprise policy related to data retention

Answer: C

Explanation:

because this would help the enterprise to comply with privacy laws and regulations by identifying and labeling the data according to its sensitivity, confidentiality, and protection requirements. Data classification can help the enterprise to apply the appropriate security controls, access rights, retention policies, and disposal methods for the data, and to prevent unauthorized or unlawful use, disclosure, or breach of the data12. Data classification can also help the enterprise to demonstrate its accountability and transparency for the data processing activities, and to meet the expectations and rights of the data subjects12.

Question: 350

Which of the following methods is MOST likely to be used to assess plausible risk scenarios that could result in reputational risk to the enterprise?

A. Controls gap analysis
B. Qualitative analysis
C. Quantitative analysis
D. SWOT analysis

Answer: B

Explanation:

Qualitative analysis is a method that uses subjective judgments and opinions to assess plausible risk scenarios that could result in reputational risk to the enterprise. Qualitative analysis can help identify the sources, causes, and impacts of reputational risk, as well as the likelihood and severity of such
risk. Qualitative analysis can also involve stakeholder feedback, surveys, interviews, focus groups, and expert opinions to evaluate the reputation of the enterprise and its IT functions.
The other options are not the most likely methods to assess plausible risk scenarios that could result in reputational risk to the enterprise. Controls gap analysis is a method that compares the existing controls with the required controls to identify any deficiencies or weaknesses that could expose the enterprise to risk. Controls gap analysis can help improve the effectiveness and efficiency of IT processes and services, but it does not directly assess the reputational risk scenarios. Quantitative analysis is a method that uses numerical data and mathematical models to measure and evaluate risk scenarios. Quantitative analysis can help estimate the financial impact and probability of risk events, but it may not capture the intangible and subjective aspects of reputational risk. SWOT analysis is a method that evaluates the strengths, weaknesses, opportunities, and threats of an organization or a project. SWOT analysis can help identify the internal and external factors that affect the performance and success of the organization or the project, but it does not specifically assess the reputational risk scenarios.

For more information on qualitative analysis and reputational risk, you can refer to these web sources: Qualitative Risk Analysis: What it is and how to implement it Reputational Risk Management: A Framework for Measurement Reputational Risk Management in IT Outsourcing: A Case Study

Question: 351

Which of the following would provide the MOST useful information to understand the associated risks when implementing a new digital transformation strategy?

A. Risk policy
B. Risk framework
C. Risk heat map
D. Risk register

Answer: C

Explanation:

Question: 352

Which of the following roles should approve major IT purchases to help prevent conflicts of interest?

A. IT steering committee
B. Chief information officer (CIO)
C. Chief compliance officer
D. Project management office (PMO)

Answer: A

Explanation:

because this is a role that should approve major IT purchases to help prevent conflicts of interest. An IT steering committee is a group of senior executives and board members who are responsible for overseeing and directing the IT function and ensuring that it aligns with the enterprise's vision, mission, goals, and strategy12. An IT steering committee should approve major IT purchases, such as hardware, software, services, or projects, to ensure that they are justified, prioritized, and aligned with the business needs and expectations, and that they deliver value and performance to the enterprise12. An IT steering committee should also ensure that the IT procurement process is transparent, fair, and ethical, and that there are no conflicts of interest or undue influence from the IT vendors or suppliers1

Question: 353

From an IT governance perspective, establishing performance measurements is PRIMARILY the responsibility of:

A. the IT architecture review board.
B. senior management.
C. the board of directors.
D. enterprise risk management (ERM).

Answer: B

Explanation:

This is because senior management is responsible for defining and communicating the IT strategy, objectives, and performance expectations for the organization. Senior management is also responsible for establishing and overseeing the IT governance framework, which includes the performance measurement metrics, processes,

and tools. Senior management should ensure that the performance measurement metrics are aligned with the business goals and value creation, as well as the IT governance principles and policies. Senior management should also monitor and evaluate the IT performance results and take corrective actions if needed.

Some of the sources that support this answer are:

1: This source explains the roles and responsibilities of senior management in IT governance, and how they can use COBIT 5 to implement effective IT governance practices. It states that senior management should define the IT-related goals and objectives, establish the ITgovernance structure and processes, assign roles and responsibilities, and ensure adequate resources and capabilities for IT governance.

2: This source discusses the importance and benefits of IT performance measurement for IT governance, and provides some tips and tools for conducting it. It suggests that senior management should be involved in setting the IT performance measurement criteria, selecting the key performance indicators (KPIs), defining the targets and thresholds, and reviewing and reporting the IT performance outcomes.

3: This source provides a comprehensive guide on how to optimize IT project intake, approval, and prioritization. It mentions that senior management should be responsible for defining the strategic alignment, value delivery, risk optimization, and resource optimization criteria for IT projects, as well as for monitoring and evaluating the IT project portfolio performance.

Question: 354

Business management is seeking assurance from the CIO that controls are in place to help minimize the risk of critical IT systems being unavailable during month-end financial processing. What is the BEST way to address this concern?

A. Create a communication plan with risk owners.
B. Outsource infrastructure hosting.
C. Restrict and monitor user access.
D. Develop key risk indicators (KRIs) and action plans.

Answer: D

Explanation:

because this would help to address the concern of business management that controls are in place to help minimize the risk of critical IT systems being unavailable during month-end financial processing. Key risk indicators (KRIs) are metrics that measure the potential impact and likelihood of the risks that may affect the IT performance and outcomes, and provide early warning signals for taking corrective actions12. Action plans are specific steps and tasks that are designed to implement the risk response strategies, such as avoiding, reducing, transferring, or accepting the risks12. Developing KRIs and action plans can help the CIO to monitor and manage the risks of IT system unavailability, and to ensure that the expected benefits and value are realized. Developing KRIs and action plans can also help to communicate and report the risk scenarios and their consequences to business management, and to demonstrate the effectiveness and efficiency of the IT controls12.

Question: 355

A root-cause analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators. Who should be accountable for resolving the situation?

A. HR training director
B. HR recruitment manager
C. Chief information officer
D. (CIO) Business process owner

Answer: C

Explanation:

The CIO is responsible for the overall IT governance and ensuring that IT supports the business objectives and strategy. The CIO should also ensure that IT staff have the necessary skills and competencies to perform their roles effectively and efficiently. The CIO should address the root cause of the service disruption and take corrective actions to prevent recurrence. Reference := CGEIT Review Manual, 27th Edition, Domain 1: Governance of Enterprise IT, page 17-18.

Question: 356

Which of the following would be the MOST effective way to ensure IT capabilities are appropriately aligned with business requirements for specific business processes?

A. Establishing key performance indicators {KPIs)
B. Requiring Internal IT architecture and design reviews
C. Requiring architecture and design reviews with business process stakeholders
D. Issuing a management mandate that IT and business process stakeholders work together

Answer: C

Explanation:

Architecture and design reviews are an effective way to ensure that IT solutions are aligned with the business requirements and objectives for specific business processes. By involving the business process stakeholders in these reviews, IT can gain a better understanding of the business needs, expectations, and constraints, as well as receive feedback and validation from the end users. This can help to avoid miscommunication, gaps, or conflicts between IT and business, and ensure that the IT

capabilities are fit for purpose and deliver value to the business. Reference := CGEIT Review Manual, 27th Edition, Domain 1: Governance of Enterprise IT, page 20-21.

Question: 357

Which of the following has PRIMARY responsibility to define the requirements for IT service levels for the enterprise?

A. The business manager
B. The help desk
C. The CIO
D. The business continuity vendor

Answer: A

Explanation:

The business manager has the primary responsibility to define the requirements for IT service levels for the enterprise, as they are the ones who understand the business needs, objectives, and expectations from the IT services. The business manager should communicate these requirements to the IT service provider, who should then design, deliver, and monitor the IT services according to the agreed service levels. The help desk, the CIO, and the business continuity vendor are not primarily responsible for defining the IT service level requirements, although they may have roles in supporting, implementing, or ensuring them. Reference := CGEIT Review Manual, 27th Edition, Domain 1: Governance of Enterprise IT, page 20-21.

Question: 358

Which of the following should be management's GREATEST consideration when trying to optimize the use of benefits from IT?

A. Value delivery
B. Quality management
C. Process improvement
D. Alignment of business to IT

Answer: A

Explanation:

Value delivery is the process of ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT. Value delivery is the greatest consideration when trying to optimize the use of benefits from IT, as it focuses on maximizing the value of IT investments and services to the business and stakeholders. Quality management, process improvement, and alignment of business to IT are important aspects of value delivery, but they are not the ultimate goal or consideration. Reference := CGEIT Review Manual, 27th Edition, Domain 1: Governance of Enterprise IT, page 21-22.

Question: 359

The use of an enterprise architecture (EA) framework BEST supports IT governance by providing:

A. key information for IT service level management.
B. reference models to align IT with business.
C. IT standards for application development
D. business information for IT capacity planning.

Answer: B

Explanation:

An enterprise architecture (EA) framework is a set of principles, guidelines, standards, and tools that help design, plan, implement, and govern the IT architecture of an enterprise. One of themain benefits of using an EA framework is that it provides reference models to align IT with business, such as the Business Architecture, the Information Systems Architecture, and the Technology Architecture. These models help define the business vision, goals, processes, information, and technology requirements of the enterprise, and ensure that they are consistent and coherent across the organization. By using an EA framework, IT governance can ensure that IT supports the business strategy, delivers value, manages risks, and optimizes resources. Reference:
What is enterprise architecture? A framework for transformation
TOGAF | opengroup.org

Question: 360

To ensure IT risk is managed in a consistent manner, it is MOST important for IT governance to establish a:

A. risk management committee to identify IT-related risks.
B. risk management framework.
C. balanced scorecard that includes IT risks.
D. risk management reporting tool to ensure compliance.

Answer: B

Explanation:

A risk management framework is a set of principles, policies, roles, responsibilities, and processes that guide, direct, and control the identification, analysis, evaluation, and treatment of IT risks. A risk management framework can help ensure that IT risk is managed in a consistent manner by: Providing a clear and coherent structure for managing IT risks across the organization
Aligning IT risks with the enterprise objectives, strategy, and risk appetite
Defining the roles and responsibilities of the IT risk owners, managers, and stakeholders Establishing the criteria and methods for assessing, prioritizing, and reporting IT risks Setting the standards and expectations for implementing and monitoring IT risk controls and responses
Ensuring the accountability and transparency of IT risk decisions and outcomes Reference:
According to the CGEIT Review Manual 2022, "A risk management framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the enterprise."1 According to the ISACA article on Understanding Cyber Risk Metrics and Reporting2, “A risk management framework provides a consistent approach to identifying, analyzing, evaluating and treating information-related risks. It also communicates the acceptable levels of risk.”
According to the NIST article on Staging Cybersecurity Risks for Enterprise Risk Management and Governance3, “A cybersecurity risk management framework is an essential tool for organizations to use in understanding their cybersecurity risks in relation to their overall organizational risks.”

Question: 361

Individual business units within an enterprise have been designing their own IT solutions without consulting the IT department. From a governance perspective, what is the GREATEST issue associated with this situation?

A. Security controls may not meet IT requirements.
B. The enterprise does not have the skills to manage the solutions.
C. The solutions conflict with IT goals and objectives.
D. The solution may conflict with existing enterprise goals.

Answer: D

Explanation:

Question: 362

The responsibility for the development of a business continuity plan (BCP) is BEST assigned to the:

A. business risk manager.
B. business owner.
C. chief executive officer (CEO).
D. IT systems owner.

Answer: B

Explanation:

IT governance is the process of ensuring that IT supports the business objectives and strategies of the enterprise, and that IT investments and resources are aligned with the enterprise’s needs and priorities. When individual business units design their own IT solutions without consulting the IT department, they may create solutions that are not compatible with the existing enterprise goals, such as customer satisfaction, operational efficiency, regulatory compliance, or innovation. This can result in duplication of efforts, waste of resources, increased complexity, security risks, or missed opportunities. Therefore, it is important for IT governance to establish a clear vision, strategy, and framework for IT that guides the business units in developing andimplementing IT solutions that support the enterprise goals. Some examples of IT governance frameworks are COBIT1, ITIL2, and ISO/IEC 385003. Reference :=

COBIT | ISACA

ITIL | AXELOS

ISO/IEC 38500:2015(en), Information technology — Governance of IT for the organization

Question: 363

Which of the following BEST demonstrates the effectiveness of enterprise IT governance?

A. An IT balanced scorecard is used.
B. Business objectives are achieved.
C. Business objectives are defined.
D. IT processes are measured.

Answer: B

Explanation:

Enterprise IT governance is the process of ensuring that IT supports the business objectives and strategies of the enterprise, and that IT investments and resources are aligned with the enterprise's needs and priorities1. The effectiveness of enterprise IT governance can be measured by the extent to which the business objectives are achieved through IT-enabled initiatives and services2. An IT balanced scorecard, business objectives definition, and IT processes measurement are all tools or activities that can help implement and monitor enterprise IT governance, but they do not demonstrate its effectiveness by themselves345.

Reference :=

IT Governance: Definition, Frameworks, and Best Practices - InvGate

The keys to effective IT governance in the digital era | CIO

Defining IT Governance and Its Roles for Business Success - ISACA

Governance of Enterprise IT - The Institute of Internal Auditors or The IIA Holistic IT Governance, Risk Management, Security and Privacy … - ISACA

Question: 364

An IT steering committee is concerned that enterprise technologies have grown stagnant and are outdated. Which of the following is the BEST strategy to invest in modern technology?

A. Decrease spending on steady state and increase spending on modernization and enhancements.
B. Redefine the target architecture to define new technologies that can be incorporated into the infrastructure.
C. Create a new investment category for innovation that becomes a new way for tracking investment decisions.
D. Update the IT human resource management plan to require training and development for emerging technologies.

Answer: C

Explanation:

One of the challenges of IT governance is to balance the competing demands of maintaining the existing IT systems and services (steady state) and investing in new technologies and capabilities (modernization and enhancements) that can support the business objectives and strategies1. A common strategy to invest in modern technology is to create a new investment category for innovation that becomes a new way for tracking investment decisions2. This category can be used to allocate funds for exploring and experimenting with emerging technologies that have the potential to create value for the enterprise, such as artificial intelligence, blockchain, internet of things, mobility, and drones3. By creating a separate category for innovation, the IT steering committee can ensure that the enterprise does not fall behind in adopting new technologies, and that the IT portfolio is aligned with the changing business needs and opportunities4. Reference := The CFO and IT:

Technology investment strategies | Deloitte Insights

Global Technology Governance Report 2021 | World Economic Forum What is IT Governance and Why Your Organization Needs It Today How CIOs Can Get IT Governance Right in an Agile World | ICF

Question: 365

The PRIMARY objective of building outcome measures is to:

A. monitor whether the chosen strategy is successful
B. visualize how the strategy will be achieved.
C. demonstrate commitment to IT governance.
D. clarify the cause-and-effect relationship of the strategy.

Answer: A

Explanation:

Outcome measures are indicators that measure the results or impacts of a strategy, program, or project on the intended beneficiaries or stakeholders1. The primary objective of building outcome measures is to monitor whether the chosen strategy is successful in achieving its goals and objectives, and to evaluate its effectiveness and efficiency2. Outcome measures can also help to communicate the value and benefits of the strategy to the relevant audiences, and to identify areas for improvement or adjustment3. Outcome measures are different from output measures, which measure the activities or products that are delivered by the strategy, but not necessarily their effects or outcomes4. Reference :=

Outcome Measures - an overview | ScienceDirect Topics

Outcome Measurement | The Australian Institute of Family Studies

Outcome Measurement: A Guide for Nonprofit Organizations | Imagine Canada Doing Quantitative Research with Outcome Measures

Question: 366

Once the strategic vision has been established, which of the following would be the BEST activity for supporting the implementation of performance measures?

A. Monitor service level performance.
B. Document strengths, weaknesses, opportunities, and threats.
C. Document policy requirements
D. Identify key performance indicators (KPIs).

Answer: D

Explanation:

Key performance indicators (KPIs) are measurable values that demonstrate how effectively an organization is achieving its key business objectives1. KPIs help to track and evaluate the progress and success of a strategy, and to communicate the results to the relevant stakeholders2. Once the strategic vision has been established, identifying KPIs would be the best activity for supporting the implementation of performance measures, because they provide a clear and quantifiable way to measure the performance of the strategy against the vision3. KPIs should be aligned with the strategic vision, relevant to the business context, specific, measurable, achievable, realistic, and time-bound4.

Reference :=

What is a Key Performance Indicator (KPI)? | Klipfolio

Key Performance Indicators (KPIs) - Definition, Types & Examples

How to Develop Key Performance Indicators - Strategy Management Group

How to Set SMART KPIs for Your Business - The Balance Small Business

Question: 367

Which of the following BEST supports the implementation of an effective data classification policy?

A. Monitoring with key performance indicators (KPIs)
B. Implementation of data loss prevention (DLP) tools
C. Clear guidelines adopted by the business
D. Classification policy approval by the board

Answer: C

Explanation:

A data classification policy is a set of rules and standards that define how data is categorized and labeled according to its sensitivity, value, and criticality for the organization1. An effective data classification policy helps to ensure that data is properly protected, accessed, and managed throughout its lifecycle2. The best way to support the implementation of an effective data classification policy is to have clear guidelines adopted by the business, because they provide a common understanding and framework for data owners, stewards, and users to classify and handle data according to the business context and requirements3. Clear guidelines also help to ensure consistency, compliance, and accountability for data classification across the organization4.

Reference :=

Data Classification Policy | Information Security Office

Data Governance and Classification Policy - University of Cincinnati

Data governance processes - Cloud Adoption Framework

Data classification in the Microsoft Purview governance portal

Question: 368

An enterprise has lost an unencrypted backup tape of archived customer data. A data breach report is not mandatory in the relevant jurisdiction. From an ethical standpoint, what should the enterprise do NEXT?

A. Initiate disciplinary proceedings against relevant employees.
B. Mandate a review of backup tape inventory procedures.
C. Communicate the breach to customers.
D. Require an evaluation of storage facility vendors.

Answer: C

Explanation:

From an ethical standpoint, the enterprise should communicate the breach to customers, because they have a right to know that their personal data has been compromised and may be at risk of identity theft, fraud, or other malicious activity. Even if the data breach report is not mandatory in the relevant jurisdiction, the enterprise has a moral duty to respect the privacy and dignity of its customers, and to be transparent and accountable for its actions. Communicating the breach to customers can also help to preserve the trust and reputation of the enterprise, and to mitigate the potential legal and financial consequences of the breach. According to some data ethics experts, data breaches should be treated as public health issues, and organizations should adopt a proactive and responsible approach to inform and protect their customers12. Some examples of data breach communication best practices are: notifying customers as soon as possible, providing clear and accurate information about the nature and extent of the breach, explaining what actions the enterprise is taking to remedy the situation and prevent future incidents, offering assistanceand support to affected customers, such as identity protection services or credit monitoring, and apologizing sincerely and expressing commitment to data ethics34.

Reference :=
Data ethics: What it means and what it takes | McKinsey
The Skeleton of a Data Breach: The Ethical and Legal Concerns
Data breaches: A public health issue? | TheHill
How to Communicate a Data Breach Effectively - IT Governance Blog

Question: 369

When developing an IT training plan, which of the following is the BEST way to ensure that resource skills requirements are identified?

A. Extract training requirements from deficiencies reported in customer service satisfaction surveys.
B. Ask managers to determine IT training requirements annually.
C. Determine training needs based on the capabilities to support the IT strategy.
D. Survey employees for IT skills requirements based upon technology trends.

Answer: C

Explanation:

An IT training plan is a document that outlines the learning objectives, activities, and resources for developing the skills and competencies of IT staff and stakeholders1. The best way to ensure that resource skills requirements are identified is to determine training needs based on the capabilities to support the IT strategy. The IT strategy is a document that defines the vision, mission, goals, and objectives of IT in alignment with the business strategy2. The IT strategy also identifies the current and future IT capabilities that are needed to deliver value and achieve the desired outcomes3. By assessing the gap between the current and future IT capabilities, the training needs can be derived and prioritized according to the IT strategy. This way, the IT training plan can ensure that the resource skills requirements are relevant, consistent, and effective for supporting the IT strategy.

Reference :=
How to Create an Effective IT Training Plan | Simplilearn
What is an IT Strategy? - Definition from Techopedia
IT Strategy: A 3-step Process To Creating Your Own
[How to Conduct a Training Needs Analysis: A Template & Example]

Question: 370

In which of the following situations is it MOST appropriate to use a quantitative risk assessment?

A. There is a lack of accurate and reliable past and present risk data.
B. The risk assessment needs to be completed in a short period of time.
C. The objectivity of the risk assessment is of primary importance.
D. The risk assessment is needed for an IT project business case.

Answer: C

Explanation:

Quantitative risk assessment is more objective than qualitative risk assessment because it uses numeric values and calculations to estimate the likelihood and impact of risks. Quantitative risk assessment is more appropriate when the risk assessment needs to be unbiased and consistent. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, p. 90-91.

Question: 371

An IT department has forwarded a request to the IT strategy committee for funding of a discretionary Investment. The committee's MOST important consideration should be to evaluate:

A. the technical feasibility of the investment.
B. the business and technical scope of the investment •
C. whether the investment supports corporate goals
D. whether the investment aligns with the enterprise architecture (EA).

Answer: C

Explanation:

Discretionary investments are those that are not mandatory or essential for the business, but may provide some benefits or opportunities. The IT strategy committee should evaluate whether the discretionary investment supports the corporate goals and aligns with the business strategy, as this is the most important criterion for IT governance and value creation. The technical feasibility, the business and technical scope, and the alignment with the EA are also important factors, but they are secondary to the strategic alignment and value proposition of the investment. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, p. 92-93; Rethinking traditional technology budgeting processes; Discretionary Investment Management Definition, Benefits & Risks.

Question: 372

Which of the following should be identified FIRST when determining appropriate IT key risk indicators (KRIs)?

A. IT-related risk
B. IT controls
C. IT threats
D. IT objectives

Answer: A

Explanation:

IT key risk indicators (KRIs) are metrics that measure the likelihood and impact of IT-related risks on the enterprise's objectives and goals. Therefore, the first step in determining appropriate IT KRIs is to identify the IT-related risks that are relevant and significant for the enterprise. IT controls, IT threats and IT objectives are also important factors in developing IT KRIs, but they are not the first step. IT controls are the measures that mitigate or reduce IT risks, IT threats are the sources of potential harm or loss to IT assets or processes, and IT objectives are the desired outcomes or results of IT activities that support the enterprise's strategy and goals. Reference := ISACA, CGEIT Review Manual, 7th Edition, 2019, p. 90-91; Integrating KRIs and KPIs for Effective Technology Risk Management; Performance Measurement Metrics for IT Governance; State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study.

Question: 373

An IT risk committee is trying to mitigate the risk associated with a newly implemented bring your own device (BYOD) policy and supporting mobile device management (MDM) tools. Which of the following would be the BEST way to ensure employees understand how to protect sensitive corporate data on their mobile devices?

A. Require staff to complete security awareness training
B. Develop security procedures for mobile devices.
C. Distribute the BYOD policy on the company Intranet.
D. Require staff to review and sign nondisclosure agreements (NDAs)

Answer: A

Explanation:

Security awareness training is the best way to ensure employees understand how to protect sensitive corporate data on their mobile devices, as it can educate them on the risks, policies, and best practices of BYOD and MDM. Security awareness training can also help employees recognize and avoid common threats, such as phishing, malware, and data leakage. Security procedures, BYOD policy, and NDAs are also important, but they are not sufficient to ensure employees have the knowledge and skills to secure their mobile devices. Security procedures and BYOD policy need to be communicated and enforced effectively, and NDAs only protect the legal rights of the organization, not the actual data on the devices. Reference := The Ultimate Guide to BYOD Security: Definition & More - Digital Guardian; What is BYOD? | IBM; How to have secure remote working with a BYOD policy; 5 Best Practices in BYOD Policy for Small Business - Scalefusion; BYOD Reignited: How To Get It Right This Time - Forbes.

Question: 374

An enterprise's decision to move to a virtualized architecture will have the GREATEST impact on:

A. system life cycle management.
B. asset classification.
C. vendor management
D. vulnerability management.

Answer: C

Explanation:

Moving to a virtualized architecture will have the greatest impact on vendor management, as it will require the enterprise to select, contract, and monitor the performance of the cloud or virtualization service providers. Vendor management is essential for ensuring that the virtualized architecture meets the enterprise's requirements, standards, and expectations, as well as for managing the risks, costs, and benefits of the virtualization strategy. Vendor management also involves negotiating and enforcing service level agreements (SLAs), ensuring compliance with regulations and policies, and resolving any issues or disputes that may arise with the vendors.

System life cycle management, asset classification, and vulnerability management are also important aspects of IT governance, but they are not as significantly affected by moving to a virtualized architecture as vendor management. System life cycle management is the process of planning, developing, testing, deploying, maintaining, and retiring IT systems. Asset classification is the process of identifying, categorizing, and labeling IT assets based on their value, sensitivity, and criticality. Vulnerability management is the process of identifying, assessing, prioritizing, and mitigating IT vulnerabilities that may pose a threat to the enterprise's security or operations. These processes may need to be adapted or updated to accommodate the virtualized architecture, but they are not fundamentally changed by it.

Reference := Steps to Meet Cloud and Virtualized Architecture Governance; Crafting the optimal model for the IT architecture organization; Enterprise Architecture Governance – Why It Is Important (Part 2); What is IT governance? A formal way to align IT & business strategy.

Question: 375

A large bank has completed several acquisitions in the last few years that have resulted in redundant IT applications. To align with the strategic initiative of providing integrated services to customers, the IT steering committee has decided to share data and integrate applications. Which of the following would be MOST important to review in this situation?

A. Enterprise architecture (EA)
B. IT risk register
C. Balanced scorecard measures
D. IT strategic plan

Answer: A

Explanation:

Enterprise architecture (EA) is the most important thing to review in this situation, as it provides a holistic view of the current and desired state of the IT applications, data, and infrastructure, as well as the business processes, capabilities, and goals that they support. EA can help identify the redundant IT applications, the data sources and dependencies, the integration requirements and challenges, and the alignment with the strategic initiative of providing integrated services to customers. EA can also help define the roadmap, standards, and governance for achieving the desired state of IT integration.

IT risk register, balanced scorecard measures, and IT strategic plan are also important things to review, but they are not as essential as EA in this situation. IT risk register is a document that records the IT risks that may affect the enterprise's objectives and operations, as well as their likelihood, impact, mitigation strategies, and status. IT risk register can help identify and manage the potential risks associated with IT integration, such as data quality, security, compatibility, performance, and compliance issues. Balanced scorecard measures are a set of metrics that track the performance of IT in relation to the enterprise's vision, strategy, and goals. Balanced scorecard measures can help evaluate the effectiveness and efficiency of IT integration, as well as its contribution to customer satisfaction, business value, and innovation. IT strategic plan is a document that outlines the vision, mission, objectives, initiatives, and actions of IT to support the enterprise's strategy and goals. IT strategic plan can help align IT integration with the business needs and expectations, as well as allocate the necessary resources and budget for it.

Reference := Enterprise Architecture Governance - CIO Wiki; Enterprise Architecture Governance | The Definitive Guide | LeanIX; Enterprise Architecture Governance – Why It Is Important (Part 2); What is IT governance? A formal way to align IT & business strategy.

Question: 376

What should be done FIRST when feedback indicates recently implemented software products are not meeting business unit expectations?

A. Review help desk logs.
B. Confirm user acceptance testing (UAT) was completed.
C. Request a gap analysis.
D. Institute a new software training program

Answer: C

Explanation:

A gap analysis is a method of assessing the differences in performance between a business' information systems or software applications to determine whether business requirements are being met and, if not, what steps should be taken to ensure they are met successfully1. A gap analysis typically involves identifying non-compliant processes or activities; assessing their risklevels; determining potential corrective actions that can be taken to address them; and implementing those corrective measures1. Once completed, organizations can then measure their progress toward achieving full compliance over time1.

A gap analysis should be done first when feedback indicates recently implemented software products are not meeting business unit expectations, as it can help identify the root causes of the dissatisfaction, the gaps between the current and desired state of the software products, and the actions needed to close those gaps. A gap analysis can also help align the software products with the business strategy, goals, and expectations, as

well as ensure compliance with regulations and policies.

Reviewing help desk logs, confirming user acceptance testing (UAT) was completed, and instituting a new software training program are also important steps to take when software products are not meeting expectations, but they are not the first step. Reviewing help desk logs can help gather feedback and identify issues or errors with the software products, but it does not provide a comprehensive analysis of the gaps and solutions. Confirming UAT was completed can help verify that the software products were tested by the end users before implementation, but it does not address the reasons why the feedback was negative after implementation. Instituting a new software training program can help improve the user's skills and knowledge of the software products, but it does not guarantee that the software products will meet their needs and expectations.

Reference := What is Gap Analysis in Compliance | Scytale; How to Perform an IT Gap Analysis - Systems X; IT Gap Analysis – First Step to ITIL Success | Invensis Learning.

Question: 377

Of the following, who is PRIMARILY responsible for applying frameworks for the governance of IT to balance the need for security controls with business requirements?

A. Data scientists
B. Data stewards
C. Data analysts
D. Data processors

Answer: B

Explanation:

Data stewards are primarily responsible for applying frameworks for the governance of IT to balance the need for security controls with business requirements, as they are the custodians of the data quality, integrity, and security within an organization. Data stewards define and implement data policies, standards, and procedures, as well as monitor and report on data compliance and performance. Data stewards also collaborate with other stakeholders, such as data owners, data users, and data scientists, to ensure that the data is aligned with the business objectives and meets the regulatory and ethical requirements.

Data scientists, data analysts, and data processors are not primarily responsible for applying frameworks for the governance of IT, as they are more focused on the technical aspects of data collection, analysis, and processing. Data scientists use advanced methods and tools to extract insights and value from data. Data analysts use descriptive and inferential statistics to explore and interpret data. Data processors perform operations on data, such as entry, validation, transformation, storage, and retrieval.

Reference := What is a Data Steward? | Informatica; Data Governance Roles: The Ultimate Guide | Collibra; Data Governance Roles: Who Does What? | erwin; [What is IT governance? A formal way to align IT & business strategy].

Question: 378

An IT steering committee is evaluating whether a third-party supplier is delivering the correct level of service Reviewing which of the following will provide the BEST information to the committee?

A. Key performance indicators (KPIs)
B. Service portfolio management
C. Vendor status reports
D. Operational cost reduction reports

Answer: A

Explanation:

Key performance indicators (KPIs) are the best source of information for the IT steering committee to evaluate whether a third-party supplier is delivering the correct level of service, as they are metrics that measure the achievement of specific goals or objectives. KPIs can help the committee assess the quality, efficiency, effectiveness, and value of the supplier's services, as well as their alignment with the enterprise's strategy and expectations. KPIs can also help the committee identify and address any issues or gaps in the supplier's performance, as well as monitor and report on their progress and improvement.

Service portfolio management, vendor status reports, and operational cost reduction reports are also useful sources of information for the IT steering committee, but they are not as comprehensive and reliable as KPIs. Service portfolio management is the process of managing the lifecycle of IT services, from conception to retirement. Service portfolio management can help the committee understand the scope, objectives, and benefits of the supplier's services, as well as their interdependencies and risks. Vendor status reports are documents that provide updates on the supplier's activities, deliverables, milestones, and issues. Vendor status reports can help the committee track and communicate the status of the supplier's services, as well as identify and resolve any problems or conflicts. Operational cost reduction reports are documents that show how the supplier's services have reduced or optimized the enterprise's operationalcosts. Operational cost reduction reports can help the committee evaluate the financial impact and return on investment (ROI) of the supplier's services.

Reference := Performance Measurement Metrics for IT Governance; KPIs for Corporate Governance Dashboard - BSC Designer; feature Performance Measurement Metrics for IT Governance - ISACA; Performance Measurement Metrics for IT Governance - ISACA.

Question: 379

Which of the following should be the PRIMARY goal of implementing service level agreements (SLAs) with an outsourcing vendor?

A. Gaining a competitive advantage
B. Establishing penalties for not meeting service levels
C. Achieving operational objectives
D. Complying with regulatory requirements

Answer: C

Explanation:

The primary goal of implementing service level agreements (SLAs) with an outsourcing vendor is to achieve operational objectives, such as improving service quality, efficiency, effectiveness, and value. SLAs are contracts that define the scope, standards, and expectations of the service delivery, as well as the roles, responsibilities, and rights of both parties. SLAs can help align the outsourcing vendor's services with the enterprise's strategy, goals, and needs, as well as monitor and measure their performance and outcomes. SLAs can also help manage the risks, costs, and benefits of outsourcing, as well as resolve any issues or disputes that may arise.

Gaining a competitive advantage, establishing penalties for not meeting service levels, and complying with regulatory requirements are possible benefits or outcomes of implementing SLAs with an outsourcing vendor, but they are not the primary goal. Gaining a competitive advantage is a strategic objective that may result from outsourcing some IT functions or processes to a vendor that can provide better or cheaper services than the enterprise itself or its competitors. Establishing penalties for not meeting service levels is a mechanism that can be included in SLAs to enforce accountability and compliance, as well as to compensate for any losses or damages caused by poor service delivery. Complying with regulatory requirements is a legal obligation that may affect the design and implementation of SLAs, especially when outsourcing involves sensitive or personal

data or cross-border transactions.

Reference := 12 Service Level Agreement (SLA) best practices for IT leaders; Contents The Complete Guide To IT Service Level Agreements - IT Governance; Service level management and service level agreements - IT Governance; Service Level Agreements: A Legal and Practical Guide.

Question: 380

An enterprise's chief information officer (CIO) has been receiving complaints from business executives regarding the amount their units are being charged for IT services. To maintain a good relationship with business peers, the CIO wants to be responsive to these complaints. To address this issue, the FIRST step should be to:

A. agree to reduce charge rates and improve relationship management with the business.
B. look into outsourcing of support functions to drive down the cost structure.
C. ask the chief financial officer (CFO) about budget revisions for the business units' IT expenditures.
D. quantify consumption and service level agreement (SLA) achievements per business unit.

Answer: D

Explanation:

The first step to address the issue of complaints from business executives regarding the amount their units are being charged for IT services should be to quantify consumption and service level agreement (SLA) achievements per business unit. This will help the CIO to understand the actual usage and performance of IT services by each business unit, as well as to justify and communicate the chargeback rates based on the value and quality of IT services delivered. Quantifying consumption and SLA achievements can also help identify and address any inefficiencies,
discrepancies, or gaps in IT service delivery or chargeback methods.
Agreeing to reduce charge rates and improve relationship management with the business, looking into outsourcing of support functions to drive down the cost structure, and asking the CFO about budget revisions for the business units' IT expenditures are possible steps to take after quantifying consumption and SLA achievements, but they are not the first step. Agreeing to reduce charge rates without understanding the underlying causes of the complaints may result in underfunding or underpricing of IT services, which may affect their quality and sustainability. Improving relationship management with the business is important, but it should be based on transparent and accurate information about IT service consumption and chargeback. Looking into outsourcing of support functions may reduce the cost structure, but it may also introduce new risks and challenges for IT governance and management. Asking the CFO about budget revisions may help align IT expenditures with business priorities, but it may not address the root causes of the dissatisfaction with IT chargeback.

Reference := IT Chargeback Drives Efficiency - Uptime Institute Blog; What is IT governance? A formal way to align IT & business strategy; Chargeback vs. IT Governance – HEIT Management.

Question: 381

Which of the following should be the FIRST action taken by a newly formed IT governance committee to ensure reports are compliant with regulations and identify key IT risks?

A. Direct the development of a reporting communication plan.
B. Develop and monitor IT key risk indicator (KRI) triggers.
C. Train end users on regulation requirements.
D. Implement a mechanism to ensure reporting escalation.

Answer: B

Explanation:

The first action taken by a newly formed IT governance committee to ensure reports are compliant with regulations and identify key IT risks should be to develop and monitor IT key risk indicator (KRI) triggers. IT KRIs are metrics that measure the likelihood and impact of IT-related risks on the enterprise's objectives and goals. IT KRI triggers are thresholds or values that indicate when a risk is approaching or exceeding an acceptable level, requiring attention or action from the IT governance committee. Developing and monitoring IT KRI triggers can help the committee to identify, prioritize, and manage IT risks, as well as to ensure compliance with regulations and policies.

Directing the development of a reporting communication plan, training end users on regulation requirements, and implementing a mechanism to ensure reporting escalation are also important actions for the IT governance committee, but they are not the first step. A reporting communication plan is a document that defines the purpose, scope, format, frequency, audience, and distribution of IT reports, as well as the roles and responsibilities of the report creators and recipients. A reporting communication plan can help the committee to communicate effectively and efficiently with the stakeholders about IT performance, issues, and risks.

Training end users on regulation requirements is a process that educates the end users on the rules and standards that apply to their use of IT systems and data, as well as the consequences of non-compliance. Training end users can help the committee to raise awareness and ensure adherence to regulations and policies. Implementing a mechanism to ensure reporting escalation is a procedure that defines the criteria, process, and channels for escalating IT reports to higher levels of authority or responsibility when necessary. Implementing a reporting escalation mechanism can help the committee to ensure timely and appropriate response and resolution of IT issues or risks.

Reference := Integrating KRIs and KPIs for Effective Technology Risk Management; Performance Measurement Metrics for IT Governance; State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study.

Question: 382

What is the BEST criterion for prioritizing IT risk remediation when resource requirements are equal?

A. Deviation from IT standards
B. IT strategy alignment
C. IT audit recommendations
D. Impact on business

Answer: D

Explanation:

The best criterion for prioritizing IT risk remediation when resource requirements are equal is the impact on business, as it reflects the potential consequences of the IT risk on the enterprise's objectives, operations, reputation, and stakeholders. The impact on business can be measured by factors such as financial loss, operational disruption, customer dissatisfaction, regulatory violation, or reputational damage. The higher the impact on business, the higher the priority for IT risk remediation.

Deviation from IT standards, IT strategy alignment, and IT audit recommendations are also important criteria for prioritizing IT risk remediation, but they are not the best criterion. Deviation from IT standards is the degree to which an IT process, system, or service does not comply with the established policies, procedures, or best practices. Deviation from IT standards can indicate a weakness or gap in IT governance or management, but it does not necessarily reflect the severity or urgency of the IT risk. IT strategy alignment is the degree to which an IT process, system, or service supports and enables the enterprise's strategy and goals. IT strategy alignment can indicate the value or importance of an IT process, system, or service, but it does not directly measure the

impact of the IT risk on the business. IT audit recommendations are the suggestions or actions proposed by an IT auditor to address the findings or issues identified during an IT audit. IT audit recommendations can provide guidance and direction for IT risk remediation, but they are not a definitive or objective criterion for prioritization.

Reference := IT Risk Management Guide for 2022 | CIO Insight; What is IT Governance, Risk, and Compliance (GRC)?; Holistic IT Governance, Risk Management, Security and Privacy: Needed for Effective Implementation and Continuous Improvement - ISACA; Cyberrisk Governance: A Practical Guide for Implementation - ISACA.

Learn more:

1. cioinsight.com2. securityscorecard.com3. isaca.org4. isaca.org5. cldigital.com+1 more

Question: 383

When developing a framework to implement IT governance, which of the following BEST contributes to the successful implementation?

A. Practical and enforceable policies
B. Automated compliance tracking
C. Comprehensive and timely audit reviews
D. Periodic peer reviews

Answer: A

Explanation:

Practical and enforceable policies are the best way to contribute to the successful implementation of a framework to implement IT governance, as they provide clear and consistent guidance and direction for IT activities, processes, and decisions. Practical and enforceable policies are based on the enterprise's strategy, goals, and values, as well as the relevant regulations and standards. Practical and enforceable policies also define the roles, responsibilities, and authorities of the IT stakeholders, as well as the mechanisms for monitoring, measuring, and reporting on IT performance and compliance. Practical and enforceable policies can help ensure that IT governance is effective, efficient, and aligned with the business needs and expectations. Automated compliance tracking, comprehensive and timely audit reviews, and periodic peer reviews are also useful ways to support the implementation of a framework to implement IT governance, but they are not the best way. Automated compliance tracking is a process that uses software tools or systems to collect, analyze, and report on IT compliance data, such as policies, standards, controls, risks, incidents, or issues. Automated compliance tracking can help reduce the time and effort required for IT compliance management, as well as improve the accuracy and reliability of IT compliance information. Comprehensive and timely audit reviews are assessments that evaluate the adequacy and effectiveness of IT governance, management, and operations. Comprehensive and timely audit reviews can help identify and address any weaknesses or gaps in IT governance, as well as provide recommendations for improvement. Periodic peer reviews are evaluations that compare the IT governance practices of an enterprise with those of its peers or competitors. Periodic peer reviews can help benchmark and improve the IT governance performance of an enterprise, as well as identify best practices or opportunities for innovation.

Reference := IT Governance: Definitions, Frameworks and Planning - ProjectManager; What is IT governance? A formal way to align IT & business strategy; What is IT Governance (ITG) and why does it matter? - IFS Blog; IT Governance Framework - CIO Wiki; What is IT Governance? How to Implement | Electric.

Question: 384

In a successful enterprise that is profitable in its marketplace and consistently growing in size, the non-IT workforce has grown by 50% in the last two years. The demand for IT staff in the marketplace is more than the supply, and the enterprise is losing staff to rival organizations. Due to the rapid growth. IT has struggled to keep

up with the enterprise, and IT procedures and associated job roles are not well-defined. The MOST critical activity for reducing the impact caused by IT staff turnover is to:

A. document processes and procedures.
B. outsource the IT operation.
C. increase compensation for IT staff
D. hire temporary staff.

Answer: A

Explanation:

The most critical activity for reducing the impact caused by IT staff turnover is to document processes and procedures, as this can help preserve the knowledge and experience of the existing IT staff, as well as facilitate the training and orientation of the new IT staff. Documenting processes and procedures can also help standardize and improve the quality and efficiency of IT operations, services, and projects, as well as ensure compliance with regulations and policies. Documenting processes and procedures can also help define and clarify the roles and responsibilities of the IT staff, as well as the expectations and requirements of the business units.

Outsourcing the IT operation, increasing compensation for IT staff, and hiring temporary staff are possible activities for addressing the IT staff turnover issue, but they are not the most critical activity. Outsourcing the IT operation may reduce the dependency on internal IT staff, but it may also introduce new risks and challenges for IT governance and management, such as vendor selection, contract negotiation, service level agreement (SLA) monitoring, and data security. Increasing compensation for IT staff may improve the retention and motivation of the existing IT staff, but it may also increase the operational costs and budget constraints of the IT department. Hiring temporary staff may fill the gaps or shortages in IT skills or resources, but it may also affect the continuity and consistency of IT service delivery, as well as the integration and collaboration of IT teams.

Question: 385

Which of the following should be done FIRST when concerns have been identified regarding the financial viability of a potential software supplier?

A. Implement an escrow agreement
B. Perform a risk assessment
C. Include a right-to-audit clause in the contract
D. License the intellectual property

Answer: B

Explanation:

A risk assessment is the process of identifying, analyzing, and evaluating the potential risks that may affect the achievement of an objective or the performance of an activity. A risk assessment should be done first when concerns have been identified regarding the financial viability of a potential software supplier, as it can help determine the likelihood and impact of the supplier's failure or default on the enterprise's IT project or operation. A risk assessment can also help identify and prioritize the mitigation strategies or contingency plans that can be implemented to reduce or avoid the negative consequences of the supplier's financial instability.

Implementing an escrow agreement, including a right-to-audit clause in the contract, and licensing the

intellectual property are possible actions to take after performing a risk assessment, but they are not the first step. An escrow agreement is a legal arrangement that involves a third party holding and releasing the software source code or other critical assets of the supplier in case of a dispute or termination of the contract. An escrow agreement can help protect the enterprise's access and rights to the software in case of the supplier's bankruptcy or insolvency. Including a right-to-audit clause in the contract is a provision that allows the enterprise to inspect and verify the financial records and statements of the supplier, as well as their compliance with the contract terms and conditions. A right-to-audit clause can help monitor and evaluate the supplier's financial performance and stability, as well as detect any fraud or misrepresentation. Licensing the intellectual property is a process that grants the enterprise a legal permission to use, modify, or distribute the software or other creations of the supplier, subject to certain limitations and obligations. Licensing the intellectual property can help secure the enterprise's ownership and control over the software, as well as prevent any infringement or violation by other parties.

Reference := How to check the viability of your suppliers; Financial Viability - Business Model Viability - Aktia Solutions; How to Assess Manufacturing Vendors' Viability; Assessing Financial Viability.

Question: 386

Which of the following is the MOST significant challenge faced by an enterprise when establishing information stewardship?

A. Lack of documented policies and procedures
B. Information requirements of regulatory authorities
C. Insufficient knowledge of IT practices and controls
D. Lack of role clarity and specific responsibilities

Answer: D

Explanation:

The most significant challenge faced by an enterprise when establishing information stewardship is the lack of role clarity and specific responsibilities, as this can lead to confusion, duplication, inconsistency, or omission of tasks and activities related to information governance. Information stewardship is the role of providing day-to-day operational support using data, such as defining and implementing data policies, standards, and procedures; monitoring and reporting on data compliance and performance; and collaborating with other stakeholders to ensure data quality, integrity, and security1. Information stewardship requires clear and consistent definition of the scope, objectives, and expectations of the role, as well as the roles and responsibilities of the information stewards and their relationship with other data owners, users, or scientists1. Withoutrole clarity and specific responsibilities, information stewardship may not be effective or efficient in achieving the desired outcomes or benefits of information governance.

Lack of documented policies and procedures, information requirements of regulatory authorities, and insufficient knowledge of IT practices and controls are also challenges faced by an enterprise when establishing information stewardship, but they are not the most significant challenge. Lack of documented policies and procedures is a challenge that can affect the standardization and improvement of information governance processes and activities, as well as the communication and enforcement of data rules and expectations. Information requirements of regulatory authorities are a challenge that can affect the compliance and accountability of information governance, as well as the protection and privacy of data. Insufficient knowledge of IT practices and controls is a challenge that can affect the technical skills and capabilities of information stewards, as well as their ability to use or integrate data systems or tools.

Reference := What is an Information Steward? | Informatica; What is an Information Steward, and Why You Should Care; What is an Information Steward, and Why You Should Care?.

Question: 387

An enterprise has decided to implement an enterprise resource planning (ERP) system to achieve operating and cost efficiencies through global IT standardization. The business units are resistant because they are used to operating autonomously. The CEO has instructed the CIO to move quickly with the implementation to force acceptance with business unit leaders. Which of the following should be the CIO's FIRST step?

A. Build a governance framework for identifying non-standard processes.
B. Request funding from the CEO to hire ERP consultants.
C. Ask the CEO to be the sponsor of the program
D. Engage a reluctant business unit to conduct a proof-of-concept pilot.

Answer: C

Explanation:

The CIO's first step should be to ask the CEO to be the sponsor of the program, as this can help overcome the resistance from the business units and ensure the support and commitment of the top management. The CEO's sponsorship can also help communicate the vision, goals, and benefits of the ERP system to the enterprise, as well as allocate the necessary resources and budget for the implementation. The CEO's sponsorship can also help resolve any conflicts or issues that may arise during the implementation, as well as monitor and evaluate the progress and outcomes of the program.

Building a governance framework for identifying non-standard processes, requesting funding from the CEO to hire ERP consultants, and engaging a reluctant business unit to conduct a proof-of- concept pilot are possible steps to take after asking the CEO to be the sponsor of the program, but they are not the first step. Building a governance framework can help define and implementthe policies, standards, and procedures for IT standardization, as well as the roles, responsibilities, and authorities of the IT stakeholders. Requesting funding can help secure the financial resources needed to hire external experts or vendors that can provide guidance and assistance for the ERP implementation. Engaging a reluctant business unit can help demonstrate the feasibility and value of the ERP system, as well as gain feedback and buy-in from the end users. However, these steps may not be effective or successful without the CEO's sponsorship and leadership.

Question: 388

Which of the following is MOST important to review during IT strategy development?

A. Industry best practices
B. IT balanced scorecard
C. Current business environment
D. Data flows that indicate areas requiring IT support

Answer: C

Explanation:

The most important thing to review during IT strategy development is the current business environment, as it reflects the internal and external factors that affect the enterprise's performance, objectives, and needs. The current business environment includes the analysis of the enterprise's strengths, weaknesses, opportunities, and threats (SWOT), as well as the assessment of the market trends, customer demands, competitor actions, and regulatory requirements. Reviewing the current business environment can help align the IT strategy with the business strategy, as well as identify and prioritize the IT initiatives and investments that can support and enable the enterprise's goals and value proposition.

Industry best practices, IT balanced scorecard, and data flows that indicate areas requiring IT support are also important things to review during IT strategy development, but they are not the most important thing. Industry best practices are the methods or techniques that have been proven to be effective or efficient in achieving a desired outcome or result in a specific domain or context. Industry best practices can help benchmark and

improve the IT strategy, as well as adopt or adapt the best solutions or innovations from other enterprises or sectors. IT balanced scorecard is a set of metrics that measure the performance of IT in relation to the enterprise's vision, strategy, and goals. IT balanced scorecard can help evaluate and communicate the effectiveness and efficiency of IT strategy, as well as its contribution to customer satisfaction, business value, and innovation. Data flows that indicate areas requiring IT support are the diagrams or models that show how data is collected, processed, stored, and distributed within or across the enterprise's processes or systems. Data flows can help identify and address the gaps or issues in IT service delivery or data management, as well as optimize or integrate the data systems or tools.

Question: 389

During an IT strategy review, a new CIO determined that numerous important internal processes have not been updated for several years and should be reexamined. Which of the following would be the BEST approach to address this concern?

A. Implement a process review policy.
B. Assemble a project review team
C. Verify that the processes are still needed
D. Map the processes to a capability maturity model.

Answer: D

Explanation:

The best approach to address the concern of outdated internal processes is to map the processes to a capability maturity model (CMM). A CMM is a framework that describes the levels of maturity and capability of a process, from initial to optimized. Mapping the processes to a CMM can help the CIO to assess the current state and performance of the processes, as well as identify and prioritize the areas for improvement. Mapping the processes to a CMM can also help align the processes with the IT strategy and goals, as well as ensure compliance with standards and best practices. Software Capability Maturity Model (CMM) | IT Governance UK provides an overview of the CMM framework and its benefits.

Implementing a process review policy, assembling a project review team, and verifying that the processes are still needed are also possible steps to take to address the concern of outdated internal processes, but they are not the best approach. Implementing a process review policy is a measure that defines the frequency, scope, criteria, and methods for reviewing and updating the processes. Implementing a process review policy can help ensure the consistency and quality of the process review activities, as well as prevent future obsolescence or inefficiency of the processes. Assembling a project review team is a task that involves selecting and assigning the roles and responsibilities of the people who will conduct or participate in the process review activities. Assembling a project review team can help ensure the availability and suitability of the resources and skills for the process review activities, as well as facilitate the collaboration and communication among the stakeholders. Verifying that the processes are still needed is a question that evaluates the relevance and value of the processes for the enterprise's objectives and operations. Verifying that the processes are still needed can help eliminate or simplify any unnecessary or redundant processes, as well as optimize or integrate any overlapping or interdependent processes.

Question: 390

When conducting a risk assessment in support of a new regulatory requirement, the IT risk committee should FIRST consider the:

A. disruption to normal business operations.
B. risk profile of the enterprise.

C. readiness of IT systems to address
D. the risk cost burden to achieve compliance.

Answer: B

Explanation:

The risk profile of the enterprise is the most important thing to consider first when conducting a risk assessment in support of a new regulatory requirement, as it reflects the overall exposure and tolerance of the enterprise to various types of risks, such as strategic, operational, financial, or compliance risks. The risk profile of the enterprise can help determine the scope, objectives, and criteria of the risk assessment, as well as the prioritization and allocation of resources and efforts for risk identification, analysis, evaluation, and treatment. The risk profile of the enterprise can also help align the risk assessment with the enterprise's strategy, goals, and values, as well as ensure consistency and integration with other risk management activities or processes. Disruption to normal business operations, readiness of IT systems to address the risk, and cost burden to achieve compliance are also important things to consider when conducting a risk assessment in support of a new regulatory requirement, but they are not the first thing to consider. Disruption to normal business operations is a potential consequence or impact of the risk on the enterprise's performance, productivity, or continuity. Disruption to normal business operations can be assessed and measured during the risk analysis or evaluation stage of the risk assessment, as well as mitigated or reduced during the risk treatment or response stage. Readiness of IT systems to address the risk is a factor that affects the capability or maturity of the enterprise's IT infrastructure, applications, or services to comply with or support the new regulatory requirement. Readiness of IT systems to address the risk can be assessed and improved during the risk treatment or response stage of the risk assessment, as well as monitored and reported during the risk communication or review stage. Cost burden to achieve compliance is a factor that affects the feasibility or affordability of the enterprise's actions or investments to comply with or support the new regulatory requirement. Cost burden to achieve compliance can be estimated and optimized during the risk treatment or response stage of the risk assessment, as well as balanced with the benefits or value of compliance.

Question: 391

Facing financial struggles, a CEO mandated severe budget cuts. A decision was also made to immediately change the enterprise strategic focus to put more reliance on mobile, cloud, and wireless services in an effort to boost revenue. The IT steering committee has asked the CIO tosuggest adjustments to the current IT project portfolio to allow support for the new direction despite fewer funds. What should the CIO advise the committee to do FIRST?

A. Ask business stakeholders to discuss their vision for the new strategy.
B. Cancel projects with a net present value (NPV) below a defined threshold.
C. Conduct a risk assessment against the potential new services.
D. Start re-allocating budget to projects involving mobile or cloud.

Answer: A

Explanation:

As this is the first step to understand the scope, objectives, and expectations of the new direction, as well as to align the IT project portfolio with the business needs and priorities. Asking business stakeholders to discuss their vision can also help identify and address any gaps or issues in the current IT project portfolio, as well as to communicate and collaborate effectively with the business units.
Canceling projects with a net present value (NPV) below a defined threshold, conducting a risk assessment against the potential new services, and starting re-allocating budget to projects involving mobile or cloud are

possible actions to take after asking business stakeholders to discuss their vision, but they are not the first step. Canceling projects with a low NPV may help free up some funds for the new direction, but it may also affect the existing or planned benefits or outcomes of those projects. Conducting a risk assessment can help evaluate the feasibility and impact of the new services, as well as identify and mitigate any threats or uncertainties. Starting re-allocating budget can help support and enable the new services, but it may also disrupt or compromise the current or ongoing projects. These actions should be based on a clear and shared understanding of the new strategy and its implications for the IT project portfolio.

Question: 392

An enterprise is approaching the escalation date of a major IT risk. The IT steering committee wants to ascertain who is responsible for the risk response. Where should the committee find this information?

A. Resource management plan
B. RACI chart
C. Risk management plan
D. Risk register

Answer: B

Explanation:

The committee should find the information about who is responsible for the risk response in the RACI chart, as this is a tool that assigns the roles and responsibilities of the stakeholders for each task or activity in a project or process. RACI stands for Responsible, Accountable, Consulted,and Informed, which are the four types of involvement or participation that a stakeholder can have in a task or activity. A RACI chart is a matrix that shows the tasks or activities as rows and the stakeholders as columns, and indicates their roles and responsibilities using the RACI codes. A RACI chart can help clarify and communicate who is doing what, who is making decisions, who is providing input, and who is being updated in a project or process1.
A resource management plan, a risk management plan, and a risk register are also important documents for managing IT risks, but they do not provide the information about who is responsible for the risk response. A resource management plan is a document that defines how the resources, such as human, financial, physical, or technological resources, will be acquired, allocated, managed, and controlled in a project or process. A resource management plan can help ensure that the resources are available and sufficient for the risk response activities. A risk management plan is a document that defines how the risks will be identified, analyzed, evaluated, treated, monitored, and communicated in a project or process. A risk management plan can help ensure that the risks are managed effectively and efficiently according to the enterprise's objectives and policies. A risk register is a document that records the risks that may affect the achievement of an objective or the performance of an activity, as well as their likelihood, impact, mitigation strategies, and status. A risk register can help identify and prioritize the risks that need to be addressed or monitored.

Question: 393

Which of the following IT governance actions would be the BEST way to minimize the likelihood of IT failures jeopardizing the corporate value of an IT-dependent organization?

A. Implement an IT risk management framework.
B. Install an IT continuous monitoring solution.
C. Define IT performance management measures.
D. Benchmark IT strategy against industry peers.

Answer: A

Explanation:

The best IT governance action to minimize the likelihood of IT failures jeopardizing the corporate value of an IT-dependent organization is to implement an IT risk management framework. An IT risk management framework is a set of policies, processes, and tools that help identify, analyze, evaluate, treat, monitor, and communicate the IT risks that may affect the achievement of the organization's objectives and goals. An IT risk management framework can help reduce the probability and impact of IT failures, such as system outages, data breaches, cyberattacks, or project delays, by implementing appropriate controls and mitigation strategies. An IT risk management framework can also help align the IT risks with the organization's riskappetite and tolerance, as well as ensure compliance with regulations and standards. What is IT Risk Management? | RSA provides an overview of IT risk management and its benefits.

Installing an IT continuous monitoring solution, defining IT performance management measures, and benchmarking IT strategy against industry peers are also useful IT governance actions, but they are not the best way to minimize the likelihood of IT failures. Installing an IT continuous monitoring solution is a process that uses software tools or systems to collect, analyze, and report on IT performance and compliance data, such as availability, reliability, security, or efficiency. Installing an IT continuous monitoring solution can help detect and respond to IT failures in a timely and effective manner, as well as improve the visibility and accountability of IT operations. Defining IT performance management measures is a task that involves selecting and defining the metrics that measure the achievement of specific goals or objectives for IT processes, systems, or services. Defining IT performance management measures can help evaluate and communicate the effectiveness and efficiency of IT operations, services, and projects, as well as their contribution to business value and customer satisfaction. Benchmarking IT strategy against industry peers is a technique that involves comparing and contrasting the IT practices, capabilities, or outcomes of an organization with those of its competitors or similar organizations. Benchmarking IT strategy against industry peers can help identify and adopt best practices or innovations for IT governance and management, as well as assess the strengths and weaknesses of the organization's IT performance.

Question: 394

Which aspect of information governance BEST enables an enterprise to avoid duplication of records and promote consistency of data?

A. Data loss prevention (DLP)
B. Data modeling
C. Blockchain management
D. Enterprise architecture (EA)

Answer: B

Explanation:

The aspect of information governance that best enables an enterprise to avoid duplication of records and promote consistency of data is data modeling. Data modeling is the process of creating and maintaining a logical representation of the data structures, relationships, and constraints that exist in an enterprise's data sources, such as databases, applications, or systems. Data modeling can help ensure that the data is accurate, complete, and standardized across the enterprise, as well as facilitate the integration, analysis, and sharing of data. Data modeling can also help improve the data quality, security, and governance, as well as support the business processes and decisions that rely on data. What is Data Modeling? Definition & Best Practices provides an overview of data modeling and its benefits.

Question: 395

The risk committee is overwhelmed by the number of false positives included in risk reports. What action would BEST address this situation?

A. Conduct a risk assessment
B. Evaluate key risk indicators (KRIs).
C. Change the reporting format.
D. Adjust the IT balanced scorecard

Answer: B

Explanation:

The best action to address the situation of the risk committee being overwhelmed by the number of false positives in risk reports is to evaluate key risk indicators (KRIs). KRIs are metrics that measure the likelihood and impact of IT-related risks on the enterprise's objectives and goals. Evaluating KRIs can help the risk committee to identify and prioritize the most significant and relevant risks, as well as to adjust the thresholds or values that trigger the risk alerts or warnings. Evaluating KRIs can also help reduce the number of false positives, which are the cases where the risk reports indicate a high level of risk, but the actual risk is low or negligible. Reducing false positives can help improve the accuracy and reliability of risk reports, as well as save time and resources for the risk committee. Conducting a risk assessment, changing the reporting format, and adjusting the IT balanced scorecard are also possible actions to take to address the situation of the risk committee being overwhelmed by false positives, but they are not the best action. Conducting a risk assessment is a process that involves identifying, analyzing, evaluating, and treating the IT risks that may affect the enterprise's objectives and operations. Conducting a risk assessment can help update and validate the risk information and data, as well as implement appropriate controls and mitigation strategies. However, conducting a risk assessment may not be sufficient or feasible to address the issue of false positives, as it may require a lot of time and effort, and it may not address the root causes of false positives, such as inaccurate or outdated KRIs. Changing the reporting format is a measure that involves modifying or improving the way that risk information and data are presented or communicated in risk reports. Changing the reporting format can help enhance and simplify the readability and usability of risk reports, as well as highlight or emphasize the key points or findings. However, changing the reporting format may not solve the problem of false positives, as it may only affect the appearance or style of risk reports, not their content or quality. Adjusting the IT balanced scorecard is a task that involves revising or updating the metrics that track the performance of IT in relation to the enterprise's vision, strategy, and goals. Adjusting the IT balanced scorecard can help evaluate and communicate the effectiveness and efficiency of IT operations, services, and projects,

as well as their contribution to customer satisfaction, business value, and innovation. However, adjusting the IT balancedscorecard may not directly address the issue of false positives, as it may focus on different aspects or dimensions of IT performance than KRIs.

Question: 396

Which of the following will BEST enable an IT steering committee to monitor the achievement of overall IT objectives on a continuous basis?

A. Defined service level agreements (SLAs)
B. Project portfolio dashboards
C. Key performance indicators (KPIs)
D. IT user survey results

Answer: C

Explanation:

Key performance indicators (KPIs) are the best way to enable an IT steering committee to monitor the achievement of overall IT objectives on a continuous basis, as they are metrics that measure the progress and

outcomes of IT activities, processes, and projects in relation to the enterprise's vision, strategy, and goals. KPIs can help the IT steering committee to assess and communicate the effectiveness and efficiency of IT operations, services, and initiatives, as well as their contribution to customer satisfaction, business value, and innovation. KPIs can also help the IT steering committee to identify and address any issues or gaps in IT performance or alignment, as well as to evaluate and improve the IT governance and management practices. Performance Measurement Metrics for IT Governance provides an overview of KPIs and their benefits for IT governance.

Defined service level agreements (SLAs), project portfolio dashboards, and IT user survey results are also useful ways to monitor the achievement of overall IT objectives, but they are not the best way. Defined SLAs are contracts that specify the scope, standards, and expectations of IT service delivery, as well as the roles, responsibilities, and rights of both the service provider and the service recipient. Defined SLAs can help ensure that the IT services meet the quality and availability requirements of the business units, as well as monitor and measure the service performance and compliance. Project portfolio dashboards are tools that display the status, progress, and performance of IT projects in a graphical or visual way. Project portfolio dashboards can help track and communicate the key information and data about IT projects, such as scope, schedule, budget, risks, or issues. IT user survey results are feedback or opinions collected from the end users of IT systems or services through questionnaires or interviews. IT user survey results can help gauge and improve the user satisfaction and experience with IT systems or services, as well as identify and address any user needs or expectations.

Question: 397

An enterprise has launched a series of critical new IT initiatives that are expected to produce substantial value Which of the following would BEST provide the board with an indication of progress of the IT initiatives?

A. Portfolio management review
B. Full life cycle cost-benefit analysis
C. Demonstration of prototype and user testing
D. Critical risk and issue walk-through

Answer: A

Explanation:

The best way to provide the board with an indication of progress of the IT initiatives is to conduct a portfolio management review. A portfolio management review is a process that involves evaluating and reporting on the performance, status, and outcomes of the IT projects, programs, and services that are part of the IT portfolio. The IT portfolio is a collection of IT investments that are aligned with the enterprise's strategic objectives and expected to produce substantial value. A portfolio management review can help the board to assess and communicate the progress of the IT initiatives, as well as to identify and address any issues or risks that may affect their success. A portfolio management review can also help the board to ensure that the IT portfolio is balanced, optimized, and aligned with the business needs and priorities. IT Portfolio Management: A Comprehensive Guide | Smartsheet provides an overview of IT portfolio management and its benefits.

Question: 398

When developing a business case for an enterprise resource planning (ERP) implementation, which of the following, if overlooked, causes the GREATEST impact to the enterprise?

A. Vendor selection
B. Salvage value of legacy hardware
C. Interdependent systems
D. IT best practices

Answer: C

Explanation:

Interdependent systems are those that rely on each other for data, functionality, or performance. If the business case for an ERP implementation overlooks the interdependencies among the existing systems, it may underestimate the complexity, cost, and risk of the project. The ERP implementation may also fail to achieve the expected benefits of integration, automation, and optimization if the interdependent systems are not properly aligned and coordinated. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version)2

Question: 399

The PRIMARY objective of IT resource planning within an enterprise should be to:

A. determine risk associated with IT resources.
B. maximize value received from IT.
C. determine IT outsourcing options.
D. finalize service level agreements (SLAs) for IT

Answer: B

Explanation:

IT resource planning is the process of identifying, allocating, and managing the IT resources needed to support the enterprise's objectives and strategies. The primary objective of IT resource planning should be to maximize the value received from IT, which means ensuring that the IT resources are aligned with the business needs, optimized for efficiency and effectiveness, and delivering the expected benefits and outcomes. IT resource planning should also consider the risks, costs, and opportunities associated with IT resources, as well as the service level agreements (SLAs) and outsourcing options that may affect the quality and availability of IT services. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), What are the Objectives of Resource Management? | Kantata2, What Is Resource Planning: A Comprehensive Guide3

Question: 400

An enterprise is replacing its customer relationship management (CRM) system with a cloud-based system. Which of the following should be done FIRST when preparing for data migration"*

A. Review the enterprise data architecture.
B. Establish a data quality plan
C. Consult the quality assurance (QA) function.
D. Acquire data migration tools.

Answer: A

Explanation:

The enterprise data architecture is the blueprint that defines how data is collected, stored, processed, integrated, and distributed within the enterprise. It also specifies the data standards, policies, rules, and models that govern the data lifecycle. Reviewing the enterprise data architecture is the first step when preparing for data migration, as it helps to identify the source and target systems, the data entities and attributes, the relationships and dependencies, the data quality and security requirements, and the potential challenges and risks of the migration. Reviewing the enterprise data architecture also helps to align the data migration with the business objectives and strategies, and to ensure that the migrated data supports

theenterprise's information needs and decision making. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), Data Architecture: A Primer for the Data Scientist, Data Migration: A Comprehensive Guide

Question: 401

A business has outsourced IT operations to several third-party providers, but service level agreements (SLAs) are not clearly defined in all cases. Which of the following is the GREATEST risk to the business?

A. Costs are not measurable.
B. Third parties could provide overlapping services.
C. The scope of work is not clearly defined.
D. Quality of services is not enforceable.

Answer: D

Explanation:

Quality of services is the degree to which the IT services meet the expectations and requirements of the customers and stakeholders. Quality of services is usually defined and measured by the service level agreements (SLAs), which are contracts that specify the service level objectives, metrics, targets, and responsibilities of both parties. If the SLAs are not clearly defined in all cases, the business faces the greatest risk of not being able to enforce the quality of services from the third- party providers. This can lead to poor performance, customer dissatisfaction, reputational damage, legal disputes, and financial losses for the business. Therefore, it is essential to have clear and comprehensive SLAs for all IT outsourcing contracts. Reference: CGEIT Exam Content Outline |

ISACA1, CGEIT Review Manual (Digital Version), Outsourcing IT: What to Expect from Your SLAs | AxiaTP2, What is an SLA? Best practices for service-level agreements | CIO1

Question: 402

An enterprise has committed to the implementation of a new IT governance model. The BEST way to begin this implementation is to:

A. identify IT services that currently support the enterprise's capability.
B. define policies for data, applications, and organization of infrastructure.
C. identify the role of IT in supporting the business.
D. prioritize how much and where to invest in IT.

Answer: C

Explanation:

The first step in implementing a new IT governance model is to identify the role of IT in supporting the business, which means clarifying the vision, mission, goals, and strategies of the enterprise and how IT can enable and align with them. This step helps to establish the businessvalue and direction of IT, as well as the expectations and responsibilities of the stakeholders involved. It also helps to define the scope and boundaries of IT governance, and to identify the key issues and challenges that need to be addressed. Identifying the role of IT in supporting the business is a prerequisite for the other steps, such as identifying IT services, defining policies, and prioritizing investments, which are based on the business needs and objectives. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), 5 Steps to Create a Governance Model to Become an IT Genius in Healthcare2

Question: 403

Which of the following should be the PRIMARY governance objective for selecting key risk indicators (KRIs) related to legal and regulatory compliance?

A. Identifying the risk of noncompliance
B. Demonstrating sound risk management practices
C. Measuring IT alignment with enterprise risk management (ERM)
D. Ensuring the effectiveness of IT compliance controls

Answer: A

Explanation:

Key risk indicators (KRIs) are metrics that measure the likelihood and impact of potential or actual risks. KRIs related to legal and regulatory compliance are designed to help the enterprise monitor and manage the risk of violating laws, regulations, standards, or ethical practices that apply to its operating environment. The primary governance objective for selecting KRIs related to legal and regulatory compliance should be to identify the risk of noncompliance, which means assessing the probability and severity of compliance breaches, as well as the root causes and consequences of such breaches. By identifying the risk of noncompliance, the enterprise can take proactive measures to prevent, mitigate, or remediate compliance issues, and to ensure that its compliance program is effective, efficient, and aligned with its business objectives and strategies. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), Compliance Metrics and KPIs For Measuring Compliance Effectiveness — RiskOptics2, 11 Key Compliance KPIs + Examples (& Why You Should Track Them …3

Question: 404

In a large enterprise, which of the following should be responsible for the implementation of an IT balanced scorecard?

A. Project management office
B. Chief information officer (CIO)
C. IT steering committee
D. Chief risk officer (CRO)

Answer: C

Explanation:

An IT steering committee is a group of senior executives and stakeholders who provide strategic direction, oversight, and guidance for IT initiatives and investments in an enterprise. An IT steering committee should be responsible for the implementation of an IT balanced scorecard, as it can ensure that the scorecard aligns with the enterprise's vision, mission, goals, and strategies, and that it reflects the needs and expectations of the customers and other stakeholders. An IT steering committee can also monitor and evaluate the performance of the IT function based on the scorecard metrics, and provide feedback and recommendations for improvement. An IT steering committee can also facilitate communication and collaboration among the IT function and other business units, and promote a culture of accountability and transparency for IT performance. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), How to implement the Balanced Scorecard: Best Practices & 10 Tips2, Who Should Manage Your Company's Balanced Scorecard?3

Question: 405

Which of the following should be established FIRST so that data owners can consistently assess the level of data protection needed across the enterprise?

A. Data encryption program
B. Data risk management program
C. Data retention policy
D. Data classification policy

Answer: D

Explanation:

A data classification policy is a plan that helps an organization determine the risk tolerance and security requirements for its data assets. A data classification policy separates data into different categories based on its sensitivity, such as public, private, or restricted. A data classification policy should be established first so that data owners can consistently assess the level of data protection needed across the enterprise, as it helps them to identify the types and locations of data they own, the potential threats and impacts of data breaches, and the appropriate security controls and measures to safeguard their data. A data classification policy also helps to ensure compliance with regulatory and legal obligations, as well as to optimize data management and governance practices. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), Data Classification Policy: Benefits, Examples, and Techniques2, Why data classification is important for security | Infosec3

Question: 406

IT maturity models measure:

A. performance.
B. value.
C. capabilities.
D. outcome.

Answer: C

Explanation:

IT maturity models measure the capabilities of an IT organization, which means the ability to perform certain activities or tasks effectively and efficiently. IT maturity models assess the current state of the IT organization in terms of people, processes, and technology, and compare it with the desired or optimal state. IT maturity models also help to identify the gaps and opportunities for improvement, and to prioritize and plan the actions to achieve higher levels of maturity. IT maturity models can be used for various purposes, such as benchmarking, strategic planning, performance management, risk management, and quality assurance. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), Use an IT maturity model - IBM Garage Practices1, IT Maturity Models, Scorecards & Assessments | Smartsheet2

Question: 407

A newly appointed CIO has been tasked with the responsibility of developing an effective IT enterprise roadmap that meets business requirements. Which of the following is the BEST way to ensure that the business needs have been taken into consideration?

A. Involve process owners in requirements gathering.
B. Implement a balanced scorecard.
C. Include user acceptance testing (UAT) as part of the resulting IT solutions.

Answer: A

Explanation:

Process owners are the individuals or groups who are responsible for the design, execution, and improvement of a business process. Process owners have a deep understanding of the business needs, goals, and challenges that the process aims to address. By involving process owners in requirements gathering, the CIO can ensure that the IT enterprise roadmap meets the business requirements and expectations, and that the IT solutions align with the business processes and outcomes. Process owners can also provide valuable feedback and insights on the feasibility, usability, and effectiveness of the IT solutions, and help to prioritize and validate the IT initiatives and deliverables. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), Definitive Guide to Developing an IT Strategy and Roadmap - CioPages2, What is a Process Owner? | Lean Six Sigma Group3

Question: 408

Right-to-audit clauses are intended to ensure the vendor: A. aligns staff skill sets adequately.

B. maintains adequate budget for risk management.
C. addresses compliance requirements.
D. optimizes IT operations for service delivery

Answer: C

Explanation:

Right-to-audit clauses are intended to ensure the vendor addresses compliance requirements, which means that the vendor follows the laws, regulations, standards, and contractual obligations that apply to their business activities and operations. Right-to-audit clauses give the contracting party the right to access and review the records, processes, or activities of the vendor to verify that they are complying with the relevant compliance requirements and that they are meeting the expectations and responsibilities outlined in the contract. Right-to-audit clauses also help to identify and mitigate any compliance risks or issues that may arise from the vendor's performance or conduct, and to enforce any corrective actions or remedies if needed. Reference: Right To Audit Clause Guide: Examples, Gotcha's & More1, Why You Should Use a Right to Audit Clause2, The Importance of Audit Rights in Vendor Contracts - Venminde

Question: 409

Which of the following should be the FIRST step for executive management to take in communicating what is considered acceptable use with regard to personally owned devices for company business?

A. Require employees to read and sign a disclaimer.
B. Develop and disseminate an applicable policy.
C. Post awareness messages throughout the facility.
D. Provide training on how to protect data on personal devices.

Answer: B

Explanation:

The first step for executive management to take in communicating what is considered acceptable use with regard to personally owned devices for company business is to develop and disseminate an applicable policy. A policy is a written set of rules and guidelines that defines the scope, objectives, roles, and responsibilities of the BYOD program. A policy also specifies the security, privacy, and usage requirements and expectations for the employees and the organization. A policy helps to establish a clear and consistent understanding of what is acceptable and unacceptable when using personal devices for work purposes, and what are the consequences

of non-compliance. A policy also helps to mitigate the potential risks and challenges associated with BYOD, such as data breaches, device loss or theft, malware infections, legal liabilities, and support issues. A policy should be developed in consultation with relevant stakeholders, such asIT, HR, legal, and business units, and disseminated to all employees through various channels, such as email, intranet, training sessions, and awareness campaigns. Reference: BYOD Policies for Organizations (4 Examples) - Dashlane1, Mobile Device Security–Bring Your Own Device (BYOD): Draft SP 1800-22 …2, Personally Owned Device Policy — FBI

Question: 410

When updating an IT governance framework to support an outsourcing strategy, which of the following is MOST important?

A. Evaluating the choice of underlying technology platforms used by the service provider
B. Ensuring the outsource provider's IT function is aligned with its business function
C. Verifying the vendor has developed standard operation procedures for outsourced functions
D. Ensuring the effective management of contracts with third-party providers

Answer: D

Explanation:

When updating an IT governance framework to support an outsourcing strategy, the most important aspect is to ensure the effective management of contracts with third-party providers. Contracts are the legal documents that define the scope, terms, conditions, and expectations of the outsourcing relationship, as well as the roles, responsibilities, and obligations of both parties. Contracts also specify the service level agreements (SLAs), key performance indicators (KPIs), and reporting mechanisms that are used to measure and monitor the quality and performance of the outsourced services. Contracts also provide the mechanisms for resolving disputes, enforcing compliance, and managing changes and risks. Therefore, ensuring the effective management of contracts with third- party providers is essential for achieving the desired outcomes and benefits of outsourcing, as well as for mitigating the potential challenges and issues that may arise from outsourcing. Reference: Outsourcing Governance Framework1, Guidelines on outsourcing arrangements2, IT governance -managing the outsourcing relationship3

Question: 411

A financial services company has implemented the use of a cloud-based centralized customer relationship management (CRM) system. The company has decided to go multi-national. Which of the following should be the enterprise risk management (ERM) committee's PRIMARY consideration?

A. Security issues
B. Vendor capability
C. Return on investment (ROI)
D. Compliance issues

Answer: D

Explanation:

Compliance issues should be the primary consideration for the ERM committee because using a cloud-based CRM system in a multi-national context may involve different legal and regulatory requirements regarding data privacy, protection, localization, and transfer. The ERM committee should ensure that the company and the cloud service provider comply with the applicable laws and standards of each country where they operate, as well as the industry-specific regulations such as PCI DSS or GDPR. Compliance issues may also affect the security, vendor capability, and ROI of the cloudbased CRM system, as non-compliance may result in fines,

penalties, reputational damage, or loss of customers. Reference:
CGEIT Review Manual 2021, Chapter 2: IT Risk Management, Section 2.3: Risk Response, page 751 CGEIT Review Questions, Answers & Explanations Manual 2021, Question 4, page 162
Cloud Compliance: What It Is + 8 Best Practices for Improving It2
Overcoming Compliance Issues in Cloud Computing | Tripwire3

Question: 412

An organization is evaluating vendors to provide mobile device management (MDM) services. Which of the following is a KEY governance consideration for the IT steering committee?

A. Service level targets align with business requirements.
B. Employee-owned devices will be covered by the service.
C. The MDM services are delivered via a cloud.
D. Technology-owned devices will be covered by the service

Answer: A

Explanation:

A key governance consideration for the IT steering committee when evaluating vendors to provide mobile device management (MDM) services is to ensure that the service level targets align with the business requirements. Service level targets are the measurable and agreed-upon levels of performance and quality that the vendor is expected to deliver for the MDM services. These targets should reflect the business needs and expectations of the organization, such as availability, reliability, security, scalability, and functionality of the MDM services. Service level targets should also be realistic, achievable, and verifiable, and should be specified in the service level agreements (SLAs) that are part of the contract with the vendor. By ensuring that the service level targets align with the business requirements, the IT steering committee can facilitate the selection of a suitable and reliable vendor that can provide effective and efficient MDM services for the organization. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), Mobile Device Management (MDM) - Gartner2, How to Set Service Level Targets for Your IT Support Team

Question: 413

IT senior management has just received a survey report indicating that more than one third of the organization's key IT staff plan to retire within the next 12 months. Which of the following is the MOST important governance action to prepare for this possibility?

A. Engage human resources (HR) for recruitment of new staff.
B. Request the development of a succession plan.
C. Review motivation drivers for key IT staff.
D. Evaluate lower-level staff as succession candidates.

Answer: B

Explanation:

A succession plan is a process of identifying and preparing potential candidates to take over key roles in an organization when the current incumbents leave or retire. A succession plan is an important governance action to prepare for the possibility of losing a large portion of the organization’s key IT staff, as it can help to ensure the continuity and stability of the IT function and its alignment with the business objectives and strategies. A succession plan can also help to mitigate the risks and challenges associated with talent shortages, knowledge gaps, and leadership transitions. A succession plan should be developed in collaboration with the human resources (HR) department, the IT senior management, and the board of directors, and should include the following steps: Identify the critical IT roles and their competencies, responsibilities, and performance

expectations Assess the current IT staff and their readiness, potential, and interest to assume higher-level or more
complex roles
Conduct a gap analysis to determine the difference between the current and future skills and capabilities needed for the IT function
Develop a talent pipeline and a talent pool of internal and external candidates who can fill the critical IT roles
Provide learning and development opportunities for the identified candidates, such as training, coaching, mentoring, job rotation, or shadowing
Monitor and evaluate the progress and performance of the candidates and provide feedback and support
Review and update the succession plan periodically to reflect any changes in the business or IT environment
Reference: Succession planning: a guide to get it right - Workable1, Succession Planning: Template, Process, Best Practices [2023] - Valamis2, Succession Planning: Best Practices - GitHub Pages3

Question: 414

A CEO wants to establish a governance framework to facilitate the alignment of IT and business strategies. Which of the following should be a KEY requirement of this framework?

A. Defined resourcing levels
B. A defined enterprise architecture (EA)
C. An outsourcing strategy
D. A service delivery Strategy

Answer: B

Explanation:

A defined enterprise architecture (EA) is a key requirement of a governance framework to facilitate the alignment of IT and business strategies. An EA is a blueprint that describes the current and future state of the organization's structure, processes, information, and technology, as well as the principles and standards that guide their design and evolution. An EA helps to align IT and business strategies by providing a common vision, language, and framework for the organization, and by ensuring that the IT investments and initiatives support the business goals and objectives. An EA also helps to optimize the performance, efficiency, and effectiveness of the IT function and its services, and to manage the risks and changes associated with IT. An EA can be developed and maintained using various methodologies and frameworks, such as TOGAF, Zachman, or FEAF.
Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), What is enterprise architecture? A framework for transformation | CIO2, Enterprise Architecture: Definition, Benefits & Examples3

Question: 415

Which of the following BEST supports enterprise decision making for IT resource allocation?

A. IT-related regulatory requirements
B. Enterprise IT strategy
C. Enterprise IT risk assessment
D. IT balanced scorecard

Answer: B

Explanation:

An enterprise IT strategy is a plan that defines the vision, mission, goals, and objectives of the IT function in relation to the business needs and expectations of the enterprise. An enterprise IT strategy also outlines the principles, policies, standards, and frameworks that guide the IT governance, management, and operations. An enterprise IT strategy best supports enterprise decision making for IT resource allocation, as it helps to align the IT resources with the business priorities and strategies, and to optimize the value and performance of the IT

function and its services. An enterprise IT strategy also helps to identify and prioritize the IT initiatives and investments that can deliver the desired outcomes and benefits for the enterprise, and to allocatethe appropriate resources for their execution and delivery. An enterprise IT strategy also helps to monitor and evaluate the results and impacts of the IT resource allocation decisions, and to provide feedback and improvement opportunities. Reference: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), What is an IT Strategy? - Definition from Techopedia2, How to create an effective IT strategy | The Enterprisers Project3

Question: 416

Which of the following is the PRIMARY responsibility of a data steward?

A. Ensuring the appropriate users have access to the right data
B. Developing policies for data governance
C. Reporting data analysis to the board
D. Classifying and labeling organizational data assets

Answer: D

Explanation:

One of the primary responsibilities of a data steward is to classify and label organizational data assets, which means to assign categories and tags to the data based on its characteristics, such as type, source, sensitivity, quality, or purpose. Classifying and labeling data helps to organize, manage, and protect the data assets, as well as to facilitate their discovery, access, and usage. Data stewards are also responsible for defining and maintaining the data classification and labeling standards and policies, and ensuring their compliance across the organization. Reference: What Is a Data Steward? Roles & Responsibilities | Zuar1, Data Stewards: Who They Are & Why Data Stewardship Matters - HubSpot Blog2, Data Steward: Roles, Responsibilities, and Certification3

Question: 417

Which of the following is MOST important for an IT strategy committee to ensure before initiating the development of an IT strategic plan?

A. Committee members are apprised of business needs
B. A risk assessment has been conducted.
C. Committee members are independent from business units.
D. IT initiatives are fully supported by the business.

Answer: A

Explanation:

According to the CGEIT exam guide, the IT strategy committee should ensure that the IT strategic plan is aligned with the business needs and goals of the enterprise. Therefore, before initiating the development of an IT strategic plan, the committee members should be apprised of the business needs and understand the expectations and requirements of the stakeholders. Reference: CGEIT Exam Candidate Guide, page 13. CGEIT Certification

Question: 418

Which of the following should senior management do FIRST when developing and managing digital applications for a new enterprise?

A. Establish an architecture review board.

B. Define the risk appetite
C. Develop key risk indicators (KRIs).
D. Implement a sourcing program.

Answer: B

Explanation:

According to the CGEIT exam guide, the risk appetite is the amount and type of risk that an enterprise is willing to accept in pursuit of its objectives. It is a key element of the IT governance framework and should be defined by senior management before developing and managing digital applications for a new enterprise. The risk appetite provides the basis for establishing the risk management strategy, policies and processes, as well as the risk culture and awareness of the enterprise. Reference: CGEIT Exam Candidate Guide, page 15. CGEIT Certification

Question: 419

To successfully implement enterprise IT governance, which of the following should be the MAIN focus of IT policies?

A. Providing business value
B. Optimizing operational benefits
C. Enhancing organizational capability
D. Limiting IT costs

Answer: A

Explanation:

According to the CGEIT exam guide, the main focus of IT policies is to provide business value by aligning IT with business objectives and strategies, ensuring effective and efficient use of IT resources, and delivering IT-enabled capabilities that meet stakeholder needs and expectations. IT policies should also support the optimization of operational benefits, the enhancement of organizational capability, and the limitation of IT costs, but these are not the main focus of IT policies. Reference: CGEIT Exam Candidate Guide, page 13. CGEIT Certification

Question: 420

An IT steering committee has received a report that supports the economic and service benefits of moving infrastructure hosting to an external cloud provider. Business leadership is very concerned about the security risk and potential loss of customer data. What is the BEST way for the committee to address these concerns?

A. Mandate there will be no customer data at rest stored on cloud servers used by the vendor.
B. Include compliance with the enterprise's data governance policy in the contract.
C. Ensure reporting and penalty clauses are included in the contract for any loss of data.
D. Require an encrypted connection between the cloud and enterprise servers.

Answer: B

Explanation:

According to the CGEIT exam guide, data governance is the set of processes that ensure that important data assets are formally managed throughout the enterprise. Data governance ensures that data can be trusted and that people can be made accountable for any adverse event that happens because of low data quality. It is

about putting people in charge of fixing and preventing issues with data so that the enterprise can become more efficient. Data governance also describes an evolutionary process for a company, altering the company's way of thinking and setting up the processes to handle information so that it may be utilized by the entire organization. When moving infrastructure hosting to an external cloud provider, it is essential to include compliance with the enterprise's data governance policy in the contract. This will ensure that the cloud provider follows the same standards and practices as the enterprise regarding data quality, security, privacy, availability, integrity and reliability. This will also help to mitigate the risk of data breaches, loss or misuse, and to protect the reputation and trust of the enterprise and its customers. Reference: CGEIT Exam Candidate Guide, page 16. CGEIT Certification, Building Cloud Governance From the Basics

Question: 421

Which of the following metrics would provide senior management with the BEST indication of the success of IT investments?

A. Number of IT investments tracked in the balanced scorecard
B. Percentage of IT investments recorded in the enterprise architecture (EA)
C. Number of IT investments impacted by business-related incidents
D. Percentage of IT investments that meet expected benefits

Answer: D

Explanation:

According to the CGEIT exam guide, the success of IT investments is measured by the extent to which they deliver the expected benefits to the enterprise and its stakeholders. Therefore, the percentage of IT investments that meet expected benefits is the best metric to indicate the success of IT investments. This metric reflects the alignment of IT with business objectives and strategies, as well as the effectiveness and efficiency of IT processes and services. The other metrics are not directly related to the success of IT investments, but rather to the management and governance of IT. Reference: CGEIT Exam Candidate Guide, page 13. CGEIT Certification, Performance Measurement Metrics for IT Governance

Question: 422

Which of the following would BEST help a CIO enhance the competencies of an IT business analytics team?

A. Understanding current staff skill sets and identifying gaps
B. Creating operational processes and identifying resources
C. Defining the IT architecture and identifying training areas
D. Establishing team goals and identifying the proper structure

Answer: A

Explanation:

According to the CGEIT exam guide, one of the roles of the CIO is to develop and maintain a high- performing IT workforce that can deliver value to the enterprise. To enhance the competencies of an IT business analytics team, the CIO should first understand the current staff skill sets and identify the gaps between the existing and desired capabilities. This will help the CIO to plan and implement appropriate training, coaching, mentoring, and career development programs for the team members. The other options are not directly related to enhancing the competencies of an IT business analytics team, but rather to other aspects of IT governance and management. Reference: CGEIT Exam Candidate Guide, page 14. CGEIT Certification, Enhancing Competencies of IT Business Analytics Team

Question: 423

Which of the following is the MOST important input for designing a development program to help IT employees improve their ability to respond to business needs?

A. Capability maturity model
B. Cost-benefit analysis
C. Skills competency assessment
D. Annual performance evaluation

Answer: C

Explanation:

According to the CGEIT exam guide, a skills competency assessment is a process of identifying and measuring the skills, knowledge and abilities of IT employees. It helps to determine the current and desired levels of proficiency for each skill, as well as the gaps and needs for improvement. A skills competency assessment is the most important input for designing a development program to help IT employees improve their ability to respond to business needs, as it provides a clear picture of the strengths and weaknesses of the IT workforce, and the areas where training, coaching, mentoring or other interventions are required. Reference: CGEIT Exam Candidate Guide, page 14. CGEIT Certification, Skills Competency Assessment

Question: 424

IT senior management is concerned that IT service levels consistently fall below those outlined in the service level agreement (SLA). Which of the following would BEST enable the CIO to build a corrective action plan?

A. Assessing the impact of the SLA failure
B. Conducting an IT performance evaluation
C. Reviewing the IT staff training plan
D. Performing a root cause analysis

Answer: D

Explanation:

According to the CGEIT exam guide, a root cause analysis (RCA) is a systematic process of identifying and analyzing the factors that cause an undesirable event or condition. It helps to determine the underlying causes of problems and issues, and to prevent their recurrence. A root cause analysis is the best way to enable the CIO to build a corrective action plan, as it provides a clear understanding of the reasons why IT service levels consistently fall below those outlined in the SLA, and suggests possible solutions and improvements. The other options are not sufficient to build a corrective action plan, as they do not address the root causes of the SLA failure. Reference: CGEIT Exam Candidate Guide, page 15. CGEIT Certification, Root Cause Analysis

Question: 425

A newly hired IT director of a large international enterprise has been asked to provide periodic updates regarding IT risk to the board. Which of the following is the MOST effective way to initially address this request?

A. Include a complete IT risk register in the monthly letter given to each board member.
B. Include key IT risks in a dashboard submitted to the board quarterly.
C. Submit a register of all IT audit findings to board members monthly.
D. Schedule quarterly meetings to discuss all open IT risks.

Answer: B

Explanation:

According to the ISACA paper on Tactics for Effectively Communicating Cybersecurity Risk to Boards of Directors1, the most effective way to initially address the request of providing periodic updates regarding IT risk to the board is to include key IT risks in a dashboard submitted to the board quarterly. A dashboard is a visual tool that can help the board members quickly understand the current status and trends of IT risk, as well as the actions taken or planned to mitigate them. A dashboard should be concise, clear, consistent and relevant, and should highlight the most significant IT risks that could impact the enterprise's objectives and performance. A dashboard should also align with the enterprise's risk appetite and tolerance, and provide recommendationsfor improvement or escalation. The other options are not as effective as a dashboard, as they may be too detailed, too frequent, too narrow or too reactive for the board's needs.

Question: 426

An assessment reveals that enterprise risk management (ERM) practices are being applied inconsistently by IT staff. Which of the following would be the MOST effective corrective action?

A. Require ERM orientation sessions
B. Request the development of an IT risk register template.
C. Request a complete skills reassessment for all IT staff.
D. Update the ERM framework.

Answer: A

Explanation:

According to the CGEIT exam guide, ERM is the process of identifying, assessing, responding to and monitoring enterprise risks in alignment with the enterprise's risk appetite and tolerance. ERM helps to ensure that the enterprise achieves its objectives and creates value for its stakeholders. To apply ERM practices consistently, IT staff need to have a common understanding of the ERM framework, principles, processes and tools that are used by the enterprise. Therefore, the most effective corrective action for an assessment that reveals inconsistent ERM practices by IT staff is to require
ERM orientation sessions. These sessions can help to educate and train IT staff on the ERM concepts, terminology, roles and responsibilities, and best practices that are relevant to their work. The other options are not as effective as ERM orientation sessions, as they do not address the root cause of the inconsistency, which is the lack of ERM knowledge and awareness among IT staff. Reference: CGEIT Exam Candidate Guide, page 15. CGEIT Certification, Enterprise-risk-management practices: Where's the evidence?

Question: 427

An enterprise's global IT program management office (PMO) has recently discovered that several IT projects are being run within a specific region without knowledge of the PMO. The projects are on time, on budget, and will deliver the proposed benefits to the specific region. Which of the following should be the PRIMARY concern of the PMO?

A. Inability to reduce the impact to the risk level of the global portfolio
B. Projects may not follow system development life cycle (SDLC)
C. Lack of control and impact to the overall PMO budget

Answer: A

Explanation:

According to the CGEIT exam guide, a global IT program management office (PMO) is responsible for overseeing and coordinating the IT projects and programs across the enterprise, ensuring alignment with the enterprise's strategy, objectives and governance framework. A PMO also helps to identify, assess, monitor and mitigate the risks associated with IT projects and programs, and to optimize the benefits and value delivered by IT investments. Therefore, the primary concern of the PMO should be the inability to reduce the impact to the risk level of the global portfolio, as this could jeopardize the overall performance and success of the enterprise's IT initiatives. If several IT projects are being run within a specific region without knowledge of the PMO, this could create potential risks such as duplication of efforts, lack of integration, inconsistency of standards and practices, misalignment of expectations and requirements, and conflicts of interests or resources. These risks could negatively affect the quality, efficiency and effectiveness of the IT projects and programs, as well as their alignment with the enterprise's strategy, objectives and governance framework. The PMO should be aware of all IT projects and programs within the enterprise, and ensure that they follow a consistent and transparent process of planning, execution, monitoring and control. The PMO should also ensure that the IT projects and programs are aligned with the enterprise's risk appetite and tolerance, and that they are regularly assessed for their risks, benefits and value. Reference: CGEIT Exam Candidate Guide, page 14. CGEIT Certification, The Role of Program Management Offices (PMOs) in Driving Business Strategy Execution

Question: 428

To evaluate IT resource management, it is MOST important to define:

A. responsibilities for executing resource management.
B. applicable key goals.
C. principles for the IT strategy.
D. IT resource utilization reporting procedures.

Answer: B

Explanation:

According to the CGEIT exam guide, IT resource management is the process of planning, acquiring, allocating, monitoring and optimizing the IT resources of an enterprise to support its strategy, objectives and goals. To evaluate IT resource management, it is most important to define the applicable key goals that the IT resources are expected to achieve or contribute to. These key goals should be aligned with the enterprise's vision, mission and values, as well as the stakeholder needs and expectations. The key goals should also be specific, measurable, achievable, relevant and timebound (SMART), and should be communicated and agreed upon by all relevant parties. Defining the applicable key goals will help to assess the performance, value and impact of IT resource management, as well as to identify the gaps, issues and opportunities for improvement. The other options are not as important as defining the applicable key goals, as they are more related to the implementation and execution of IT resourcemanagement, rather than its evaluation. Reference: CGEIT Exam Candidate Guide, page 14. CGEIT Certification, IT Resource Management

Question: 429

A newly appointed CIO has issued a new IT strategic plan. Which of the following is the MOST effective way for the CIO to ensure the IT management team is held accountable for the delivery of the plan?

A. Update the IT balanced scorecard with key objectives.
B. Enforce disciplinary action for managers if the plan is not delivered.
C. Revise the managers' performance goals to include key objectives.
D. Provide management training on IT Strategic Objectives

Answer: C

Explanation:

The most effective way for the CIO to ensure the IT management team is held accountable for the delivery of the plan is to revise the managers' performance goals to include key objectives that are aligned with the IT strategic plan. This way, the managers will have clear and measurable targets that reflect their contribution to the IT strategy and vision. The CIO can also monitor and evaluate the managers' progress and performance based on these goals, and provide feedback, recognition, or improvement actions as needed.
The other options are not the most effective way for the CIO to ensure the IT management team is held accountable for the delivery of the plan. Updating the IT balanced scorecard with key objectives is a good practice, but it does not directly link the objectives to the managers' individual responsibilities and incentives. Enforcing disciplinary action for managers if the plan is not delivered is a negative and punitive approach, which may demotivate and discourage the managers from pursuing the plan. Providing management training on IT strategic objectives is a helpful initiative, but it does not specify how the managers will be assessed and rewarded for achieving the objectives. For more information on IT strategic planning and accountability, you can refer to these web sources: IT Strategic Planning: A Step-by-Step Guide How to Hold Your Team Accountable
IT Governance - CIO Wiki

Question: 430

An enterprise has entered into a new market which brings additional regulatory compliance requirements. What should be done FIRST to address these requirements?

A. Outsource the compliance process.
B. Appoint a compliance officer.
C. Update the organization's risk profile.
D. Have executive management monitor compliance.

Answer: C

Explanation:

According to the CGEIT exam guide, the organization's risk profile is a representation of the current and potential risks that the organization faces, as well as the likelihood and impact of those risks. The risk profile helps to inform the risk management strategy, policies and processes, as well as the risk appetite and tolerance of the organization. When an enterprise enters into a new market that brings additional regulatory compliance requirements, the first thing that should be done is to update the organization's risk profile to reflect the new sources, types and levels of risk that the enterprise may encounter. This will help to identify and assess the compliance risks, as well as to plan and implement appropriate risk responses and controls. The other options are not the first things that should be done, as they are more related to the execution and monitoring of compliance, rather than the identification and assessment of compliance risks.
Reference: CGEIT Exam Candidate Guide, page 15. CGEIT Certification, How to Develop a Risk Profile

Question: 431

Which of the following is the MOST important benefit of effective IT governance reporting?

A. The enterprise balanced scorecard is aligned with IT dashboards.
B. Business executives better understand IT's value contribution to the enterprise
C. IT key performance indicators (KPIs) are included in the enterprise-level KPI dashboard.
D. IT processes are improved in line with business requirements.

Answer: B

Explanation:

According to the ISACA paper on IT Governance Reporting1, the most important benefit of effective IT governance reporting is that it helps business executives better understand IT's value contribution to the enterprise. IT governance reporting is the process of communicating relevant and reliable information about the performance, value and risk of IT to the stakeholders who are responsible for making decisions and taking actions related to IT. Effective IT governance reporting enables business executives to have a clear and comprehensive view of how IT supports and enables the achievement of the enterprise's strategy, objectives and goals. It also helps business executives to assess the alignment, efficiency and effectiveness of IT, as well as to identify and address the gaps, issues and opportunities for improvement. Effective IT governance reporting fosters trust, collaboration and accountability between business and IT, and enhances the reputation and credibility of IT within the enterprise. The other options are not as important as business executives better understanding IT's value contribution to the enterprise, as they are more related to the means or outcomes of effective IT governance reporting, rather than the benefit itself. Reference: IT Governance Reporting

Question: 432

A large enterprise has been experiencing high turnover of skilled IT personnel, resulting in a significant loss of knowledge within the IT department. Which of the following is the BEST
governance action to address this concern?

A. Update the IT resource management plan.
B. Revise IT strategic objectives.
C. Update IT employee compensation packages.
D. Mandate the use of employee contracts.

Answer: A

Explanation:

According to the CGEIT exam guide, the IT resource management plan is a document that describes how the IT resources of an enterprise will be acquired, allocated, monitored and optimized to support the IT strategy, objectives and goals. The IT resource management plan should also address the human resource aspects of IT, such as recruitment, retention, development, motivation and performance of IT personnel. Therefore, the best governance action to address the concern of high turnover of skilled IT personnel is to update the IT resource management plan to reflect the current and future needs and challenges of the IT department. The updated IT resource management plan should include strategies and actions to reduce the turnover rate, such as improving the IT work environment and culture, offering competitive compensation and benefits packages, providing career development and training opportunities, enhancing employee engagement and recognition, and implementing knowledge management and succession planning practices. Reference: CGEIT Exam Candidate Guide, page 14. CGEIT Certification, IT Resource Management, Employee Turnover Rate: Definition & Calculation

Question: 433

The PRIMARY reason a CIO and IT senior management should stay aware of the business environment is to:

A. revisit prioritization of IT projects.
B. adjust IT strategy as needed.
C. measure efficiency of IT resources.
D. re-assess the IT investment portfolio.

Answer: B

Explanation:

According to the CGEIT exam guide, the primary reason a CIO and IT senior management should stay aware of the business environment is to adjust IT strategy as needed. IT strategy is the plan that defines how IT will support and enable the business strategy and objectives of the enterprise. The business environment is the external and internal factors that affect theenterprise's performance and success, such as market trends, customer demands, competitor actions, regulatory changes, technological innovations, etc. The CIO and IT senior management should stay aware of the business environment to identify and anticipate the opportunities and threats that may arise, and to align and adapt the IT strategy accordingly. This will help to ensure that IT delivers value, benefits and competitive advantage to the enterprise, and that IT risks are managed and mitigated effectively. Reference: CGEIT Exam Candidate Guide, page 13. CGEIT Certification, What is IT Strategy?, What is Business Environment?

Question: 434

Which of the following decisions would be made by the IT strategy committee?

A. Communication plan for a major IT initiative
B. Cloud implementation and support plan
C. Enterprise risk management (ERM) framework
D. Composition of the investment portfolio

Answer: D

Explanation:

According to the ISACA paper on IT Governance Reporting1, the IT strategy committee is a boardlevel committee that is responsible for overseeing and guiding the IT strategy and governance of the enterprise. The IT strategy committee helps to ensure that IT supports and enables the achievement of the enterprise's strategy, objectives and goals, and that IT delivers value, benefits and competitive advantage to the enterprise. One of the decisions that would be made by the IT strategy committee is the composition of the investment portfolio, which is the set of IT projects and programs that are selected, prioritized, funded and monitored by the enterprise. The composition of the investment portfolio reflects the strategic alignment, value proposition and risk profile of IT, as well as the resource allocation and optimization of IT. The other options are not decisions that would be made by the IT strategy committee, but rather by other IT governance bodies or roles, such as the IT steering committee, the IT management team, or the chief information officer (CIO). Reference: IT Governance Reporting, IT Strategy Committee

Question: 435

Which of the following BEST enables an enterprise to determine how business expectations should be addressed in a governance program?

A. Business impact analysis (BIA)
B. Cost-benefit analysis
C. Enterprise risk analysis
D. Stakeholder analysis

Answer: D

Explanation:

This is because stakeholder analysis is a process of identifying and prioritizing the people or groups who have an interest, influence, or impact on the enterprise's objectives and activities. Stakeholder analysis can help to

understand the business expectations, needs, preferences, and concerns of different stakeholders, as well as their roles and responsibilities in the governance program.

Stakeholder analysis can also help to engage and communicate with stakeholders effectively, and to align the governance program with the business strategy and value creation.

Some of the sources that support this answer are:

1: This source explains the importance and benefits of stakeholder analysis for IT governance, and provides some tips and tools for conducting it. It suggests that stakeholder analysis can help to ensure that IT governance meets stakeholder needs, delivers value, and supports business objectives.

2: This source defines stakeholder analysis and describes its steps and techniques. It also provides some examples of stakeholder analysis templates and matrices that can be used for IT governance projects.

3: This source discusses how stakeholder analysis can be used in the TOGAF framework for enterprise architecture. It states that stakeholder analysis should be used during Phase A (Architecture Vision) to identify the key players in the engagement, and also be updated throughout each phase; different stakeholders may be uncovered as the engagement progresses through into Opportunities & Solutions, Migration Planning, and Architecture Change Management.

4: This source presents a chapter on enterprise governance of IT processes from a book titled "Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5". It mentions that stakeholder analysis is one of the key activities for defining the IT governance framework, as it helps to identify the relevant stakeholders and their expectations, roles, and responsibilities.

Question: 436

The CIO of a financial and insurance company is considering the projects and portfolio for the coming year Which of the following projects is a non-discretionary project?

A. Data center relocation
B. Compliance with statutory regulations
C. Actuarial application system analysis and design
D. Core banking applications scalability assessment

Answer: B

Explanation:

According to the web search results, projects where management has a choice in implementing them are called discretionary projects. Projects where no choice exists are called nondiscretionary projects1. Compliance with statutory regulations is a nondiscretionary project, as it is required by law and cannot be avoided or postponed. The other options are discretionary projects, as they are based on the management's decision and preference, and can be prioritized or delayed according to the business needs and goals. Reference: CGEIT Certification, CIO Dashboard, Answers

Question: 437

Which of the following is MOST important to include in IT governance reporting to the board of directors?

A. Critical risks
B. Technology cost savings
C. Threat landscape
D. Security events

Answer: A

Explanation:

According to the ISACA paper on IT Governance Reporting1, the most important information to include in IT governance reporting to the board of directors is the critical risks that IT faces or poses to the enterprise. Critical risks are those that have a high likelihood and impact, and that could threaten the achievement of the enterprise's strategy, objectives and goals. Critical risks could include cyberattacks, data breaches, regulatory compliance violations, IT project failures, IT service disruptions, IT resource shortages, etc. The board of directors should be aware of the critical risks, as well as the actions taken or planned to mitigate them. The other options are not as important as
critical risks, as they are more related to the operational or tactical aspects of IT, rather than the strategic or governance aspects.

Question: 438

A business unit is planning to replace an existing IT legacy solution with a hosted Software as a Service (SaaS) solution. However, business management is concerned that stored data will be at risk. Which of the following is the MOST effective way to reduce the risk associated with the SaaS solution?

A. Research the technology and identify potential security threats.
B. Include risk-related requirements in the SaaS contract.
C. Create key risk indicators (KRIs) for the SaaS solution.
D. Redefine the risk appetite and risk tolerance.

Answer: B

Explanation:

According to the web search results, a SaaS contract is a legal agreement between a SaaS provider and a customer that defines the terms and conditions of using the SaaS solution, such as the scope, duration, price, service level, data ownership, security, privacy, compliance, etc. The most effective way to reduce the risk associated with the SaaS solution is to include risk-related requirements in the SaaS contract, such as the following12:

The SaaS provider should comply with the relevant laws and regulations that apply to the customer's industry and location, such as GDPR, HIPAA, PCI DSS, etc.
The SaaS provider should implement adequate security measures and controls to protect the customer's data from unauthorized access, modification, disclosure or loss, such as encryption, authentication, authorization, backup, etc.
The SaaS provider should provide regular reports and audits on the security and performance of the SaaS solution, as well as notify the customer of any security incidents or breaches that may affect the customer's data.
The SaaS provider should guarantee a certain level of availability and reliability of the SaaS solution, and specify the remedies or penalties for any service downtime or disruption.
The SaaS provider should allow the customer to access, export, delete or transfer their data at any time, and ensure that the data are erased or returned to the customer upon termination of the contract.
The SaaS provider should indemnify and hold harmless the customer from any claims, damages or liabilities arising from the use of the SaaS solution.
Including risk-related requirements in the SaaS contract will help to clarify the roles and responsibilities of both parties, as well as to establish trust and accountability between them. It will also help to mitigate the potential risks and challenges of using a hosted SaaS solution34, such as data loss, unauthorized access, compliance violations, service outages, vendor lock-in, etc. The other options are not as effective as including risk-related requirements in the SaaS contract, as they do not address the contractual and legal aspects of using a hosted SaaS solution.

Question: 439

A project sponsor has circumvented the request for proposal (RFP) selection process. Which of the following is the MOST likely reason for this control gap?

A. Inadequate stage-gate reviews
B. Inadequate board oversight
C. Lack of accountability for policy adherence
D. Lack of a legal and regulatory review process

Answer: C

Explanation:

According to the web search results, a request for proposal (RFP) is a formal document that solicits proposals from potential vendors for a product or service. The RFP process is intended toensure a fair, transparent and objective selection of the best vendor that meets the requirements and expectations of the project sponsor and the enterprise. The RFP process typically involves the following steps1:

Planning and preparation: Define the scope, objectives, budget, timeline and evaluation criteria of the project. Identify the stakeholders and decision makers involved in the RFP process. Research the market and potential vendors. Develop the RFP document that outlines the project details, requirements, expectations and instructions for the vendors.

Issuing and advertising: Distribute the RFP document to the potential vendors, either directly or through public channels. Provide a deadline for submitting proposals and a contact person for inquiries. Advertise the RFP opportunity to attract more qualified vendors.

Receiving and reviewing: Receive the proposals from the vendors by the deadline. Review and evaluate the proposals based on the predefined criteria, such as technical capabilities, experience, references, pricing, etc. Shortlist the most suitable vendors for further consideration.

Negotiating and awarding: Conduct negotiations with the shortlisted vendors to clarify any questions, concerns or issues. Discuss the terms and conditions of the contract, such as scope, deliverables, schedule, payment, etc. Select the best vendor that offers the most value and benefit to the project and the enterprise. Award the contract to the chosen vendor and notify the other vendors of the decision.

Managing and monitoring: Manage and monitor the performance and progress of the vendor throughout the project lifecycle. Ensure that the vendor meets the contractual obligations and delivers quality results on time and within budget. Provide feedback and support to the vendor as needed. Resolve any conflicts or disputes that may arise.

A project sponsor who circumvents the RFP selection process violates the established policies and procedures of the enterprise, as well as undermines the integrity and credibility of the RFP process. The most likely reason for this control gap is a lack of accountability for policy adherence, which means that there is no clear assignment of roles and responsibilities for following and enforcing the policies, or no effective mechanisms for monitoring and reporting policy compliance, or no adequate consequences for policy violations. A lack of accountability for policy adherence can lead to poor governance, increased risk, reduced value and damaged reputation for both the project sponsor and the enterprise23. Therefore, it is essential to establish and maintain a strong culture of accountability for policy adherence within the enterprise, as well as to implement appropriate controls and measures to ensure compliance with policies. Reference: The RFP process: The Ultimate Step-by-Step Guide, Criteria and Methodology for GRC Platform Selection, The Ultimate RFP Guide: Steps, Guidelines & Template, Guidebook: Crafting a Driven Request for Proposals (RFP)

Question: 440

An enterprise is adopting a new governance framework. Of the following, the MOST effective method to help ensure that key activities are performed by appropriate resources is through the use of:

A. a RACI chart.
B. an organizational breakdown structure.
C. a work breakdown structure.

Answer: A

Explanation:

A RACI chart is a matrix that defines the roles and responsibilities of different stakeholders in a project or process. RACI stands for Responsible, Accountable, Consulted and Informed. A RACI chart can help ensure that key activities are performed by appropriate resources by clarifying who is responsible for doing the work, who is accountable for the outcome, who needs to be consulted for input or feedback, and who needs to be informed of the progress or results. Reference: ISACA, Reporting Cybersecurity Risk to the Board of Directors, page 8.

Question: 441

To enable IT to deliver adequate services and maintain availability of a web-facing infrastructure, an IT governance committee should FIRST establish:

A. web operations procedures.
B. business continuity plans (BCPs).
C. key performance indicators (KPIs).
D. customer survey processes.

Answer: C

Explanation:

Key performance indicators (KPIs) are metrics that help measure the performance of IT service delivery and align it with the business goals and stakeholder expectations. KPIs can help the IT governance committee to monitor, evaluate and improve the availability, quality and efficiency of the web-facing infrastructure. KPIs can also help identify and address any issues or risks that may affect the service level agreements (SLAs) or customer satisfaction. KPIs should be established before implementing other measures such as web operations procedures, business continuity plans (BCPs) or customer survey processes, as they provide the basis for setting objectives, targets and benchmarks for these measures. Reference: ISACA, Performance Measurement Metrics for IT Governance, page 11. datapine, Top 20 IT KPIs - Explore The Best IT KPI Examples & IT Metrics

Question: 442

What should be an IT steering committee's FIRST course of action when an enterprise is considering establishing a virtual reality store to sell its products?

A. Request a resource gap analysis.
B. Request development of key risk indicators (KRIs).
C. Request a threat assessment.
D. Request a cost-benefit analysis.

Answer: D

Explanation:

A cost-benefit analysis (CBA) is a process that evaluates the costs and benefits of a project or investment to determine its feasibility and profitability for an organization. A CBA can help the IT steering committee to compare different options for establishing a virtual reality store, such as the required hardware, software, data center, security, marketing, maintenance, etc. A CBA can also help estimate the potential

revenues, customer satisfaction, competitive advantage, and social impact of the virtual reality store. A CBA can provide a rational basis for decision-making and prioritization of the project. A CBA should be requested before other actions such as a resource gap analysis, a key risk indicator (KRI) development, or a threat assessment, as they depend on the scope and objectives of the project that are defined by the CBA. Reference: ISACA, Performance Measurement Metrics for IT Governance, page 11. ProjectManager, Cost-Benefit Analysis: A Quick Guide with Examples and Templates2. HBS Online, Cost-Benefit Analysis: What It Is & How to Do It

Question: 443

Which of the following should occur FIRST in the IT investment process?

A. Assess each project's impact on the enterprise's investment plan.
B. Select IT projects that will best support the enterprise's mission.
C. Analyze IT investments based on past data.
D. Analyze the risks and benefits of the investment for each IT project.

Answer: B

Explanation:

The IT investment process is a systematic approach to selecting, managing, and evaluating information technology investments that align with the enterprise's strategic goals and objectives. The first step in the IT investment process is to select IT projects that will best support the enterprise's mission, vision, and values. This involves identifying the business needs, problems, or opportunities that IT can address, and prioritizing them based on their alignment with the enterprise's strategy, performance, and risk management. This step also involves defining the scope, objectives, and expected outcomes of each IT project, and establishing criteria for measuring its success and value. Selecting IT projects that will best support the enterprise's mission helps ensure that IT investments are relevant, effective, and efficient for the enterprise.

Question: 444

Which of the following should be done FIRST when designing an IT balanced scorecard?

A. Develop key performance indicators (KPIs).
B. Communicate to stakeholders
C. Analyze the business strategy.
D. Review the IT resource plan.

Answer: C

Explanation:

An IT balanced scorecard (BSC) is a tool that helps align IT goals and performance with the business strategy and vision. The first step in designing an IT BSC is to analyze the business strategy and understand its objectives, priorities, and challenges. This will help identify the key stakeholders, customers, and value propositions of the IT function, as well as the critical success factors and risks that affect IT performance. Analyzing the business strategy will also help define the scope and purpose of the IT BSC, and establish the linkages between the IT goals and the business goals.

Analyzing the business strategy should be done before developing key performance indicators (KPIs), communicating to stakeholders, or reviewing the IT resource plan, as these steps depend on the clarity and alignment of the business strategy.

Question: 445

An IT strategy committee wants to ensure stakeholders understand who owns each strategic objective. To enable this understanding, which of the following should be communicated to stakeholders?

A. A RACI chart
B. The strategic plan
C. Performance measure
D. Risk owners

Answer: A

Explanation:

A RACI chart is a tool that assigns roles and responsibilities for each strategic objective, using the acronym RACI to denote who is Responsible, Accountable, Consulted, and Informed for each objective. A RACI chart can help stakeholders understand who owns each strategic objective, who is involved in its execution, and who needs to be updated on its progress and outcomes. A RACI chart can also help avoid confusion, duplication, or conflict among stakeholders, and ensure clear communication and accountability for each objective.

Question: 446

Which of the following are the MOST important processes for information asset life cycle management?

A. Procurement management and third-party management
B. Configuration management and financial management
C. Vulnerability management and network management
D. Business continuity management and disaster recovery management

Answer: D

Explanation:

Business continuity management (BCM) and disaster recovery management (DRM) are the most important processes for information asset life cycle management, as they ensure the availability, integrity, and security of information assets in the event of a disruption or disaster. BCM and DRM involve identifying the critical information assets, assessing the potential threats and impacts, developing and implementing plans and procedures to prevent, respond to, and recover from incidents, testing and reviewing the plans and procedures regularly, and ensuring the alignment of the plans and procedures with the business objectives and stakeholder expectations. BCM and DRM help protect the information assets from loss, damage, corruption, theft, or unauthorized access, and enable the organization to resume its normal operations as quickly as possible after a disruption or disaster.

Question: 447

Which of the following is the BEST way to implement effective IT risk management?

A. Align with business risk management processes.
B. Establish a risk management function.
C. Minimize the number of IT risk management decision points.
D. Adopt risk management processes.

Answer: A

Explanation:

Effective IT risk management is not a standalone process, but rather a part of the overall business risk

management framework. IT risks are interrelated with business risks, and they can affect the achievement of business objectives and strategies. Therefore, IT risk management should align with business risk management processes, such as identifying, assessing, prioritizing, treating, monitoring, and reporting risks. Aligning IT risk management with business risk management processes can help ensure that IT risks are considered in the context of the business environment, that IT risk appetite and tolerance are consistent with the business risk appetite and tolerance, that IT risk responses are aligned with the business risk responses, and that IT risk performance is communicated to the relevant stakeholders. Aligning IT risk management with business risk management processes can also help optimize the use of resources, enhance the value of IT investments, and improve the governance and accountability of IT risks.

Question: 448

Which of the following is a PRIMARY responsibility of the CIO when an enterprise plans to replace its enterprise resource applications?

A. Reviewing the IT application portfolio
B. Evaluating and selecting application vendors
C. Ensuring IT architecture requirements are considered
D. Establishing software quality criteria

Answer: C

Explanation:

The CIO is the chief information officer of an enterprise, who oversees and optimizes the use of information technology (IT) to achieve the business objectives and strategy. One of the primary responsibilities of the CIO is to ensure that IT architecture requirements are considered when an enterprise plans to replace its enterprise resource applications (ERAs). ERAs are integrated software systems that support various business functions, such as finance, accounting, human resources, supply chain, etc. IT architecture requirements are the specifications and standards that define how the IT systems and platforms should be designed, developed, deployed, and maintained to support the ERAs and their users. IT architecture requirements include aspects such as performance, scalability, security, reliability, interoperability, usability, etc. The CIO should ensure that IT architecture requirements are considered when an enterprise plans to replace its ERAs, because they can affect the quality, efficiency, and effectiveness of the ERAs and their alignment with the business needs and goals. The CIO should also ensure that the IT architecture requirements are consistent with the enterprise's IT strategy and vision, and that they comply with the relevant policies, regulations, and best practices.

Topic 3, Exam pool C

Question: 449

A CIO is planning to interview enterprise stakeholders to assess whether the IT strategic plan is continuing to support enterprise business objectives. The CIO would be MOST effective by starting the interview process with:

A. the executive team.
B. the internal auditors.
C. senior IT managers.
D. business process owners.

Answer: A

Explanation:

The executive team consists of the senior leaders of the enterprise, such as the CEO, CFO, COO, etc. They are

responsible for setting the vision, mission, goals, and strategy of the enterprise, andfor overseeing its performance and governance. The CIO is part of the executive team and should align the IT strategic plan with the enterprise business objectives. Therefore, the CIO would be most effective by starting the interview process with the executive team, as they can provide the most relevant and authoritative input on the enterprise's direction, priorities, challenges, and expectations. The executive team can also help the CIO gain support and approval for the IT strategic plan from other stakeholders, such as the internal auditors, senior IT managers, and business process owners. Reference: ISACA, Reporting Cybersecurity Risk to the Board of Directors, page 81. ISACA, Performance Measurement Metrics for IT Governance, page 1

Question: 450

Which of the following characteristics would BEST indicate that an IT process is a good candidate for outsourcing?

A. Strategic processes that require expert professionals
B. Processes with higher risk to the enterprise
C. Non-strategic processes that are not documented
D. Operational processes that are well-defined

Answer: D

Explanation:

Operational processes are the routine and repetitive tasks that support the day-to-day operations of an enterprise, such as data entry, payroll, customer service, etc. These processes are usually well- defined, standardized, and measurable, which makes them easier to outsource to a third-party provider who can perform them more efficiently and cost-effectively. Outsourcing operational processes can also free up internal resources and capabilities for more strategic and innovative activities that add value to the enterprise. Therefore, operational processes that are well-defined are a good candidate for outsourcing. Reference: ISACA, The Outsourcing Handbook A guide to outsourcing1. Time Doctor, The clear & complete guide to IT outsourcing (2023)2. Tutorial-Reports.com, Criteria for selecting an outsourcing vendor3

Question: 451

A CIO wants to make improvements to the enterprise's IT governance. Which of the following would BEST help to demonstrate the expected benefits from proposed changes?

A. RACI chart
B. Balanced scorecard
C. Enterprise architecture (EA)
D. Business case

Answer: B

Explanation:

A balanced scorecard (BSC) is a tool that helps measure and communicate the performance of an organization or a function in relation to its strategy and objectives. A BSC typically includes four perspectives: financial, customer, internal process, and learning and growth. A BSC can help a CIO to make improvements to the enterprise's IT governance by defining the IT vision, mission, goals, and metrics that align with the business needs and expectations. A BSC can also help demonstrate the expected benefits from proposed changes by showing how they will affect the IT performance indicators and outcomes in each perspective. A BSC can provide a clear and comprehensive picture of the current and desired state of IT governance, as well as the gaps and opportunities for improvement.

Question: 452

An IT team is having difficulty meeting new demands placed on the department as a result of a major and radical shift in enterprise business strategy. Which of the following is the CIO's BEST course of action to address this situation?

A. Utilize third parties for non-value-added processes.
B. Align the business strategy with the IT strategy.
C. Review the current IT strategy.
D. Review the IT risk appetite.

Answer: B

Explanation:

According to the CGEIT exam content outline1, one of the subtopics under the domain of Governance of Enterprise IT is "Governance Strategy Alignment with Enterprise Objectives". This subtopic covers the process of ensuring that the IT strategy is aligned with the business strategy and supports the achievement of enterprise goals and objectives. Therefore, the best course of action for the CIO in this situation is to align the business strategy with the IT strategy, which would help the IT team to meet the new demands and deliver value to the enterprise. Reference: 1: CGEIT Exam Content Outline | ISACA

Question: 453

An organization has decided to integrate IT risk with the enterprise risk management (ERM) framework. The FIRST step to enable this integration is to establish:

A. a common risk management taxonomy.
B. a common risk organization.
C. common key risk indicators (KRIs).
D. common risk mitigation strategies.

Answer: A

Explanation:

A common risk management taxonomy is a set of terms and definitions that are used consistently across the enterprise to describe, measure, and report on risks. A common risk management taxonomy is essential for integrating IT risk with the ERM framework, as it enables a common understanding of risk concepts, categories, and levels among different stakeholders and functions. A common risk management taxonomy also facilitates the aggregation and comparison of risks across the enterprise, and supports the alignment of risk appetite and tolerance with business objectives12. Reference: 1: Integrated Enterprise IT Risk Management (ERM) Programs - CohnReznick3 2: Introducing Risk Taxonomy - ISACA4

Question: 454

The BEST way for a CIO to manage the organizational impact of deploying a new enterprise-wide tool is to implement:

A. change management.
B. project management.
C. risk management.
D. resource management.

Answer: A

Explanation:

Change management is the process of planning, implementing, and managing the human side of change in an organization. Change management aims to minimize the resistance and disruption caused by a change, and maximize the adoption and benefits of the change1. Deploying a new enterprise-wide tool is a significant change that affects the way people work, communicate, and collaborate. Therefore, the best way for a CIO to manage the organizational impact of this change is to implement change management practices, such as:

Assessing the readiness and impact of the change on the stakeholders

Developing a communication and engagement plan to inform and involve the affected parties Providing training and support to help the users learn and use the new tool

Measuring and monitoring the progress and outcomes of the change Reinforcing and sustaining the change through feedback and recognition Project management, risk management, and resource management are also important aspects of deploying a new enterprise-wide tool, but they are not sufficient to address the human side of change. Project management focuses on delivering the project on time, on budget, and on scope2. Risk management identifies, analyzes, and mitigates the potential threats and opportunities associated with the project3. Resource management allocates and optimizes the use of human, financial, and physical resources for the project4. However, none of these processes directly deal with the behavioral and emotional aspects of change, such as overcoming resistance, building commitment, and creating a culture of change. Therefore, change management is the best way for a CIO to manage the organizational impact of deploying a new enterprise-wide tool.

Reference: 1: What is Change Management? - Prosci 2: What is Project Management? | PMI 3: What is Risk Management? | PMI 4: What is Resource Management? | PMI

Question: 455

An enterprise recently approved a bring your own device (BYOD) policy. The IT steering committee has directed IT management to develop a communication plan to disseminate information regarding the associated technical risks. Which of the following is MOST important to include in this communication plan?

A. A link on the corporate intranet to the BYOD policy
B. Potential exposures and impacts using common terms
C. Schedule and content for mandatory training
D. Disciplinary actions for violation of the BYOD policy

Answer: B

Explanation:

A communication plan is a document that outlines the objectives, strategies, tactics, and messages for communicating with a specific audience. A communication plan for disseminating information regarding the technical risks of BYOD should include the following elements12:

The purpose and goals of the communication

The target audience and their needs and preferences

The key messages and tone of the communication

The communication channels and methods

The roles and responsibilities of the communicators

The timeline and frequency of the communication

The evaluation and feedback mechanisms

The most important element to include in this communication plan is the key messages, which should convey the potential exposures and impacts of BYOD using common terms that the audience can understand. The key messages should explain what BYOD is, why it is important, what are the benefits and challenges, what are the risks and threats, how to protect the devices and data, and what are the best practices and policies. The key messages should also be consistent, clear, concise, relevant, and engaging12.

Watermark Sample

The other options are not as important as the key messages, as they are either supporting or secondary elements of the communication plan. A link on the corporate intranet to the BYOD policy is a communication channel, which is a means of delivering the message, but not the message itself. A schedule and content for mandatory training is a communication tactic, which is a specific action or activity to implement the strategy, but not the strategy itself. Disciplinary actions for violation of the BYOD policy is a message detail, which is a specific piece of information to support the message, but not the message itself.

Reference: 1: How to Write a Communication Plan: A Start-to-Finish Guide3 2: How to Create a Communication Plan (with Pictures) - wikiHow4

Question: 456

Which of the following will BEST enable an enterprise to convey IT governance direction and objectives?

A. Skills and competencies
B. Principles and policies
C. Corporate culture
D. Business processes

Answer: B

Explanation:

Principles and policies are the best way to convey IT governance direction and objectives, as they provide a clear and consistent framework for decision making, behavior, and actions in the organization. Principles are the fundamental statements that guide the IT governance process and reflect the values and beliefs of the organization. Policies are the specific rules and procedures that implement the principles and ensure compliance with the IT governance objectives12.

Skills and competencies are the abilities and knowledge that enable the IT staff to perform their roles and responsibilities effectively. They are important for achieving IT governance objectives, but they do not convey them directly. Skills and competencies are developed through training, education, and experience3.

Corporate culture is the shared set of norms, beliefs, and values that influence the behavior and attitudes of the organization's members. Corporate culture can support or hinder IT governance, depending on how well it aligns with the IT governance objectives. Corporate culture is influenced by leadership, communication, and incentives4.

Business processes are the activities and tasks that deliver value to the organization's customers and stakeholders. Business processes are aligned with the IT governance objectives to ensure efficiency, effectiveness, and quality. Business processes are designed, executed, monitored, and improved using various methods and tools5.

Reference: 1: What is IT governance? A formal way to align IT & business strategy | CIO1 2: IT Governance: Definition, Frameworks, and Best Practices - InvGate2 3: IT Governance Framework in ITSM - KnowledgeHut4 4: Corporate governance of information technology - Wikipedia3 5: What Is IT Governance? Definition, Practices and Frameworks5

Question: 457

Which of the following is the MOST important reason that IT strategic planning processes need to be adequately documented and communicated?

A. To justify spending on IT projects
B. To promote transparency to stakeholders
C. To ensure other departments are aligned with the direction set by IT
D. To inform business units of IT department achievements

Answer: B

Explanation:

IT strategic planning processes need to be adequately documented and communicated for several reasons, but the most important one is to promote transparency to stakeholders. Transparency means being open, honest, and accountable for the actions and decisions of the IT department. Transparency helps to build trust, credibility, and confidence among the stakeholders, such as senior management, business units, customers, suppliers, regulators, and employees1. By documenting and communicating the IT strategic planning processes, the IT department can demonstrate how it aligns its goals and objectives with the business strategy, how it prioritizes and executes its projects and initiatives, how it measures and reports its performance and outcomes, and how it manages its risks and challenges. Documenting and communicating the IT strategic planning processes also enables the IT department to solicit feedback and input from the stakeholders, and to address any issues or concerns that may arise23.

The other options are not as important as promoting transparency to stakeholders. Justifying spending on IT projects is a benefit of documenting and communicating the IT strategic planning processes, but it is not the primary reason. Ensuring other departments are aligned with the direction set by IT is a result of documenting and communicating the IT strategic planning processes, but it is not the main purpose. Informing business units of IT department achievements is a part of documenting and communicating the IT strategic planning processes, but it is not the most important reason.

Reference: 1: Creating an IT Strategy Communications Plan: 5 Keys to Success4 2: IT Strategy Template for a Successful Strategic Plan | Gartner1 3: 14 Ways To Document Communications Processes For Faster … - Forbes

Question: 458

Which of the following is the PRIMARY responsibility of a data steward at an enterprise with mature data management programs?

A. Implementing processes for data collection and use
B. Ensuring compliance with data privacy laws and regulations
C. Establishing data quality requirements and metrics
D. Developing data-related policies and procedures

Answer: C

Explanation:

A data steward is a functional role in data management and governance, with responsibility for ensuring that data policies and standards turn into practice within the steward's domain. Data stewards assist the enterprise in leveraging domain data assets to full capacity1. One of the primary responsibilities of a data steward is to establish data quality requirements and metrics, which define the criteria and measures for assessing the fitness of data for its intended use. Data quality requirements and metrics are based on the business needs and expectations of the data consumers, and they cover various dimensions of data quality, such as accuracy, completeness, consistency, timeliness, validity, and reliability23. Data stewards also monitor and report on the data quality performance, identify and resolve data quality issues, and implement continuous improvement initiatives to enhance the data quality4.

The other options are not the primary responsibility of a data steward, especially at an enterprise with mature data management programs. Implementing processes for data collection and use is a responsibility of a data engineer or a data analyst, who design and execute the technical aspects of data acquisition, transformation, storage, and analysis5. Ensuring compliance with data privacy laws and regulations is a responsibility of a data protection officer or a data privacy officer, who oversee the legal and ethical aspects of data processing,

security, and consent. Developing data-related policies and procedures is a responsibility of a data governance committee or a data governance officer, who set the strategic direction and objectives for data management and governance across the enterprise.

Reference: 1: What Is a Data Steward? Roles & Responsibilities | Zuar2 2: Data Quality Requirements: Definition & Examples - Talend 3: Data Quality Metrics: Definition & Examples - Talend 4: 6 Key Responsibilities of the Invaluable Data Steward - Dun & Bradstreet1 5: Data Engineer vs. Data Analyst: What's The Difference? - Simplilearn : What is a Data Protection Officer (DPO)? Learn About the Role & Responsibilities | Varonis : What is Data Governance? Definition, Best Practices & More | Collibra

Question: 459

An enterprise recently implemented a significant change in its business strategy by moving to a technologically advanced product with considerable impact on the business. What should be the FINAL step in completing the changes to IT processes?

A. Updating the configuration management database (CMDB)
B. Empowering the business to embrace the changes
C. Ensuring a return to stabilized business operations
D. Updating the enterprise architecture (EA)

Answer: C

Explanation:

According to the web search results, IT change management is the process of tracking and managing a change throughout its entire life cycle, from start to closure, with the aim to minimize risk1. One of the steps in the IT change management process is to collect and analyze data, quantify gaps and understand resistance, and modify the plan as needed2. The final step in completing the changes to IT processes is to ensure a return to stabilized business operations, which means that the change has been successfully implemented and the expected benefits have been realized3. This step also involves closing the change request, documenting the lessons learned, and celebrating the achievements4.

The other options are not the final step in completing the changes to IT processes, but rather intermediate steps that occur before or during the change implementation. Updating the configuration management database (CMDB) is a step that occurs during the change implementation, as it involves recording and tracking the changes made to the IT assets and services. Empowering the business to embrace the changes is a step that occurs before and during the change implementation, as it involves providing communication, training, and support to help the stakeholders adopt and adapt to the changes. Updating the enterprise architecture (EA) is a step that occurs before or during the change implementation, as it involves aligning the IT strategy, processes, and systems with the business goals and requirements.

Reference: 1: IT change management: A comprehensive guide - ManageEngine1 2: What is Change Management? Organizational, Process, Definition … - ASQ3 3: The Evolution of IT Change Management | Atlassian2 4: What is IT Change Management? - ServiceNow4 : What is Configuration Management Database (CMDB)? | ServiceNow : What is Organizational Change Management? | Prosci : What is Enterprise Architecture? | Gartner

Question: 460

When selecting a cloud provider, which of the following provides the MOST comprehensive information regarding the current status and effectiveness of the provider's controls?

A. Globally recognized certification
B. Third-party audit report
C. Control self-assessment (CSA)
D. Maturity assessment

Answer: B

Explanation:

A third-party audit report is the most comprehensive source of information regarding the current status and effectiveness of a cloud provider's controls. A third-party audit report is an independent and objective assessment of the cloud provider's security, compliance, and performance by a qualified and reputable auditor. A third-party audit report can provide assurance to the cloud customers that the cloud provider has implemented adequate and effectivecontrols to meet the industry standards and best practices, as well as the contractual obligations and customer expectations12.

A globally recognized certification is a credential that demonstrates that a cloud provider has met certain criteria or standards for security, quality, or performance. A globally recognized certification can provide some level of confidence to the cloud customers that the cloud provider has achieved a minimum level of compliance or competence, but it may not provide enough details or evidence about the current status and effectiveness of the cloud provider's controls3.

A control self-assessment (CSA) is a process that enables a cloud provider to evaluate its own controls internally, without involving an external auditor. A CSA can help a cloud provider to identify and address any gaps or weaknesses in its controls, as well as to monitor and improve its performance. However, a CSA may not provide sufficient assurance to the cloud customers, as it may lack objectivity, transparency, and validity4.

A maturity assessment is a process that measures the level of maturity or capability of a cloud provider's processes or practices. A maturity assessment can help a cloud provider to benchmark its performance against industry standards or best practices, as well as to identify areas for improvement or innovation. However, a maturity assessment may not provide enough information about the current status and effectiveness of the cloud provider's controls, as it may focus more on the process rather than the outcome5.

Reference: 1: Cloud Security Auditing: Challenges and Emerging Approaches - IEEE Journals & Magazine1 2: Cloud Security Audit: What You Need to Know | CloudHealth by VMware2 3: Cloud Security Certifications: What You Need to Know | CloudHealth by VMware3 4: Control SelfAssessment - ISACA4 5: Maturity Assessment - ISACA

Question: 461

Which of the following is the BEST way to encourage employees to raise ethics concerns in full confidence?

A. Publish and enforce a code of conduct policy.
B. Provide access to legal resource benefits.
C. Establish and communicate a whistle-blower policy.
D. Provide protection language in employment contracts.

Answer: C

Explanation:

A whistle-blower policy is a document that defines how ethics violations should be reported and how the whistle-blowers should be protected from retaliation. A whistle-blower policy is the best way to encourage employees to raise ethics concerns in full confidence, as it provides them with a clear, safe, and confidential channel to voice their concerns and seek resolution. A whistle-blower policy also demonstrates the organization's commitment to ethical conduct and accountability, and fosters a culture of trust and openness12.

The other options are not as effective as establishing and communicating a whistle-blower policy. Publishing and enforcing a code of conduct policy is important for defining the ethical standards and expectations for the organization, but it does not necessarily encourage employees to raise ethics concerns, unless it is

accompanied by a whistle-blower policy that ensures their protection and support3. Providing access to legal resource benefits is helpful for employees who need legal advice or assistance, but it does not guarantee their confidence or safety in reporting ethics violations, especially if they fear retaliation from their employer or co-workers4. Providing protection language in employment contracts is useful for safeguarding the rights and interests of employees, but it may not be sufficient or specific enough to address the issues and challenges faced by whistle-blowers, such as harassment, discrimination, or termination5.

Reference: 1: Here's What You Need in Your Whistleblower Policy (and Why) - Case IQ4 2: Whistle Blowing in the Public Sector - Markkula Center for Applied Ethics3 3: Ethics Policies vs. Whistleblower Policies - What's the Difference? - CMS1 4: Legal Resources | Employee Benefits | The Hartford 5: Whistleblower Protection: Overview of Federal Laws | Congressional Research Service

Question: 462

What is the PRIMARY benefit of aligning information architecture with enterprise architecture (EA)?

A. It improves communication with senior management and the business.
B. It ensures the adoption of enterprise data quality standards.
C. It enables the tracing of data to business functions.
D. It facilitates appropriate access to data consumers.

Answer: C

Explanation:

Information architecture is the design and organization of data and information assets in an enterprise, such as databases, documents, metadata, and taxonomies. Enterprise architecture (EA) is the holistic view and planning of the business strategy, processes, systems, and technology in an enterprise, such as business architecture, application architecture, data architecture, and technology architecture1. Aligning information architecture with EA means ensuring that the data and information assets are consistent, coherent, and supportive of the EA goals and objectives2.

The primary benefit of aligning information architecture with EA is that it enables the tracing of data to business functions, which means that the data can be linked to the business processes, activities, roles, and outcomes that use or produce it. This benefit has several advantages for the enterprise, such as34:

Improving data quality, accuracy, and reliability by identifying and resolving any data issues or gaps in the business functions

Enhancing data governance, security, and compliance by defining and enforcing the data policies and standards for the business functions

Increasing data value, usability, and accessibility by providing the data consumers with relevant and timely data for their business functions

Supporting data-driven decision making and innovation by enabling the analysis and evaluation of data for the business functions

The other options are not the primary benefit of aligning information architecture with EA, but rather secondary or potential benefits. Improving communication with senior management and the business is a benefit of EA in general, but not specific to information architecture alignment. Ensuring the adoption of enterprise data quality standards is a benefit of data governance, which may be facilitated by information architecture alignment, but not guaranteed. Facilitating appropriate access to data consumers is a benefit of data security and privacy, which may be improved by information architecture alignment, but not directly.

Reference: 1: What is Enterprise Architecture? | Gartner1 2: Aligning Information Architecture with Business Strategy - DATAVERSITY2 3: The Benefits of Enterprise Architecture in Organizational …3 4: An Enterprise Architecture Approach for Assessing the Alignment Between

Question: 463

A CIO is planning to implement an enterprise resource planning (ERP) system at the request of the business. Of the following, who is accountable for providing sponsorship for the IT-enabled change across the enterprise?

A. CEO
B. Human resource (HR) director
C. IT strategy committee
D. CIO

Answer: A

Explanation:

According to the web search results, the CEO is accountable for providing sponsorship for the IT- enabled change across the enterprise. The CEO is the highest-ranking executive in the organization, and has the authority and responsibility to lead the strategic direction and vision of the enterprise. The CEO also has the power and influence to allocate resources, prioritize initiatives, resolve conflicts, and communicate with stakeholders. Therefore, the CEO is the best person to provide sponsorship for the ERP implementation, which is a major and complex IT-enabled change that affects the entire enterprise12.

The other options are not as accountable as the CEO for providing sponsorship for the IT-enabled change across the enterprise. The HR director is responsible for managing the human resources functions of the organization, such as recruitment, training, compensation, and performance management. The HR director may support the ERP implementation by facilitating change management, employee engagement, and organizational development, but does not have the same level of authority and accountability as the CEO3. The IT strategy committee is a group of senior executives from different business units that provide guidance and oversight for the IT strategy and governance of the organization. The IT strategy committee may advise and approve the ERP implementation, but does not have the same level of leadership and visibility as the CEO4. The CIO is responsible for managing the IT functions of the organization, such as planning, implementing, and operating the IT systems and services. The CIO may lead and execute the ERP implementation, but does not have the same level of responsibility and influence as the CEO.

Reference: 1: What Is A Project Sponsor & Do You Need One When Implementing ERP?1 2: Building a Successful ERP Implementation Team | NetSuite2 3: What Does an HR Director Do? | Indeed.com 4: What Is an IT Strategy Committee? | Bizfluent : What is a CIO? Everything you need to know about the Chief Information Officer explained | ZDNet

Question: 464

Which of the following is MOST important to include in the customer dimension of an IT balanced scorecard?

A. Business value creation
B. Stakeholder satisfaction
C. Maintenance of IT operations
D. Support for corporate customers

Answer: B

Explanation:

According to the web search results, the customer dimension of an IT balanced scorecard is the perspective that measures how well the IT department meets the needs and expectations of its internal and external customers, such as business units, end users, suppliers, and partners. The customer dimension helps the IT

department to align its services and products with the customer requirements and preferences, and to deliver value and satisfaction to the customers12.

The most important measure to include in the customer dimension of an IT balanced scorecard is stakeholder satisfaction, which is the degree to which the customers are satisfied with the quality, performance, and outcomes of the IT services and products. Stakeholder satisfaction reflects the customer perception and feedback of the IT department, and influences the customer loyalty, retention, and advocacy. Stakeholder satisfaction can be measured by various methods, such as surveys, interviews, focus groups, complaints, compliments, and referrals34.

The other options are not as important as stakeholder satisfaction to include in the customer dimension of an IT balanced scorecard. Business value creation is a measure that belongs to the financial dimension of an IT balanced scorecard, as it evaluates how much value the IT department contributes to the business strategy and objectives5. Maintenance of IT operations is a measure that belongs to the internal process dimension of an IT balanced scorecard, as it assesses how well the IT department manages and improves its core processes and activities. Support for corporate customers is a measure that belongs to the learning and growth dimension of an IT balanced scorecard, as it indicates how well the IT department develops and enhances its capabilities and competencies to support its customers.

Reference: 1: The customer perspective within the Balanced Scorecard3 2: The Balanced Scorecard Customer Perspective2 3: Customer Satisfaction: A Guide for Measuring Customer Satisfaction - Qualtrics4 4: How to Measure Customer Satisfaction: Do You Overlook these 4 Key Customer Satisfaction Measurements? | Qualtrics 5: The financial perspective within the Balanced Scorecard : The internal process perspective within the Balanced Scorecard : The learning & growth perspective within the Balanced Scorecard

Question: 465

A CIO has recently been made aware of a new regulatory requirement that may affect IT-enabled business activities. Which of the following should be the CIO s FIRST step in deciding the appropriate response to the new requirement?

A. Revise initiatives that are active to reflect the new requirements.
B. Confirm there are adequate resources to mitigate compliance requirements.
C. Consult with legal and risk experts to understand the requirements.
D. Consult with the board for guidance on the new requirements

Answer: C

Explanation:

The CIO’s first step in deciding the appropriate response to the new regulatory requirement should be to consult with legal and risk experts to understand the requirements. This step is important because the legal and risk experts can provide the CIO with the relevant and accurate information about the new regulation, such as its scope, objectives, implications, and deadlines. The legal and risk experts can also advise the CIO on the potential risks and impacts of non-compliance, as well as the best practices and strategies for compliance .

The other options are not the first step in deciding the appropriate response to the new regulatory requirement, but rather subsequent steps that depend on the outcome of the consultation with the legal and risk experts. Revising initiatives that are active to reflect the new requirements is a step that occurs after the CIO has understood the requirements and assessed their impact on the current IT-enabled business activities. Confirming there are adequate resources to mitigate compliance requirements is a step that occurs after the CIO has identified and prioritized theactions and tasks needed to achieve compliance. Consulting with the board for guidance on the new requirements is a step that occurs after the CIO has developed and proposed a feasible and effective compliance plan. Reference: : How to Respond to Regulatory Changes - Smartsheet : Regulatory Change Management: A Guide for Compliance Teams | LogicGate

Question: 466

Which of the following BEST enables effective enterprise risk management (ERM)?

A. Risk register
B. Risk ownership
C. Risk tolerance
D. Risk training

Answer: B

Explanation:

According to the CGEIT exam content outline1, one of the subtopics under the domain of Risk Optimization is "Risk Ownership and Accountability". This subtopic covers the process of assigning and communicating the roles and responsibilities for risk management to the appropriate stakeholders, such as business owners, process owners, or risk owners. Risk ownership is the best way to enable effective enterprise risk management (ERM), as it ensures that the risks are identified, assessed, treated, monitored, and reported by the people who have the authority, knowledge, and interest to manage them. Risk ownership also fosters a risk-aware culture and promotes accountability and transparency for risk management23.

The other options are not as effective as risk ownership to enable ERM. A risk register is a tool that records and tracks the information about the risks, such as their description, category, impact, likelihood, status, and action plan. A risk register is useful for documenting and communicating the risks, but it does not ensure that the risks are managed properly by the responsible parties4. A risk tolerance is a measure that defines the acceptable level of variation from the expected outcome or objective. A risk tolerance is important for setting the boundaries and criteria for risk management, but it does not guarantee that the risks are aligned with the business strategy and objectives5. A risk training is a program that provides education and awareness on risk management concepts, methods, and tools. A risk training is beneficial for enhancing the skills and competencies of the risk management staff and stakeholders, but it does not ensure that they perform their roles and responsibilities effectively6.

Reference: 1: CGEIT Exam Content Outline | ISACA1 2: Risk Ownership - ISACA2 3: Risk Ownership: The First Step in Enterprise Risk Management - ERM3 4: What Is a Risk Register? Explanation & Free Template - ProjectManager.com 5: What Is Risk Tolerance? Definition & Examples - Talend 6: IT Risk Management Training | ISACA

Question: 467

Which of the following BEST supports an IT staff restructure as part of an annual IT strategy review with senior management?

A. Established IT key performance indicators (KPIs)
B. IT staff training program requirements
C. External IT staffing benchmarks
D. An updated business case for IT resourcing

Answer: D

Explanation:

An updated business case for IT resourcing is a document that provides the rationale and justification for the proposed changes in the IT staff structure, such as the number, roles, skills, and costs of the IT personnel. An updated business case for IT resourcing should align with the IT strategy and objectives, as well as the business needs and expectations. An updated business case for IT resourcing should also include the benefits, risks, and impacts of the IT staff restructure, as well as the alternatives and recommendations12.

The other options are not as effective as an updated business case for IT resourcing to support an IT staff restructure. Established IT key performance indicators (KPIs) are measures that evaluate the performance and outcomes of the IT department, such as service quality, customer satisfaction, project delivery, and innovation. Established IT KPIs are important for monitoring and reporting the IT results and achievements, but they do not necessarily support an IT staff restructure, unless they are linked to the proposed changes in the IT staff structure3. IT staff training program requirements are specifications that define the learning needs and objectives of the IT personnel, such as skills development, knowledge enhancement, and career advancement. IT staff training program requirements are beneficial for improving the capabilities and competencies of the IT staff, but they do not directly support an IT staff restructure, unless they are aligned with the new roles and responsibilities of the IT personnel4. External IT staffing benchmarks are standards or best practices that compare the IT staff structure of other organizations or industries, such as staffing ratios, skill levels, or salary ranges. External IT staffing benchmarks are useful for assessing and improving the competitiveness and efficiency of the IT department, but they do not adequately support an IT staff restructure, unless they are customized and adapted to the specific context and situation of the organization5.

Reference: 1: How to Write a Business Case: 4 Steps to a Perfect Business Case Template - ProjectManager.com 2: How to Write a Business Case — 4 Steps to a Perfect Business Case Template | Workfront 3: 18 Key Performance Indicator (KPI) Examples Defined - ClearPoint Strategy 4: How to Create an Effective Training Program: 8 Steps to Success - Convergence Training Blog 5: How to Benchmark Your Staffing Levels - HR Daily Advisor

Question: 468

Which of the following is the BEST critical success factor (CSF) to use when changing an IT value management program in an enterprise?

A. Documenting the process for the board of directors' approval
B. Adopting the program by using an incremental approach
C. Implementing the program through the enterprise's change plan
D. Aligning the program to the business requirements

Answer: D

Explanation:

Aligning the program to the business requirements. IT value management is the process of planning, measuring, and optimizing the value delivered by IT to the business. Changing an IT value management program means introducing new or improved methods, tools, or practices to enhance the IT value management process. The best CSF for this change is to align the program to the business requirements, which means ensuring that the program supports the business strategy, goals, and needs, and delivers the expected benefits and outcomes to the business stakeholders12. The other options are not as effective as aligning the program to the business requirements to use as a CSF for changing an IT value management program. Documenting the process for the board of directors' approval is a step that may be required for changing an IT value management program, but it does not guarantee that the program will be successful or effective. Adopting the program by using an incremental approach is a strategy that may help to implement the change more smoothly and gradually, but it does not ensure that the change will meet the business expectations or needs. Implementing the program through the enterprise's change plan is a tactic that may facilitate the coordination and communication of the change across the enterprise, but it does not ensure that the change will align with the business strategy or goals.

Reference: 1: IT Value Management - Compact3 2: 7 Rules for Demonstrating the Business Value of IT - Gartner

Question: 469

What should be the FIRST action of a new CIO when considering an IT governance framework for an enterprise?

A. Understand corporate culture and IT'S role in providing business value.
B. Understand critical IT processes to define the scope of the IT governance framework.
C. Verify stakeholder sponsorship of the IT governance initiative.
D. Develop an IT balanced scorecard to monitor and track IT performance.

Answer: A

Explanation:

This action is important because corporate culture is the shared set of norms, beliefs, and values that influence the behavior and attitudes of the organization's members. Corporate culture can support or hinder IT governance, depending on how well it aligns with the IT governance objectives. IT's role in providing business value is the extent to which IT contributes to the achievement of the business strategy, goals, and needs. IT's role in providing business value can vary depending on the industry, market, and competitive environment of the enterprise12.

By understanding corporate culture and IT's role in providing business value, the new CIO can gain insight into the current state and challenges of IT governance in the enterprise, as well as the expectations and requirements of the stakeholders. The new CIO can also identify the gaps and opportunities for improvement or innovation in IT governance, and develop a vision and strategy for IT governance that is aligned with the corporate culture and business value34.

The other options are not the first action of a new CIO when considering an IT governance framework for an enterprise, but rather subsequent actions that depend on the outcome of understanding corporate culture and IT's role in providing business value. Understanding critical IT processes to define the scope of the IT governance framework is a step that occurs after the new CIO has established the objectives and priorities for IT governance, and needs to determine which processes are essential for delivering value and managing risk5. Verifying stakeholder sponsorship of the IT governance initiative is a step that occurs after the new CIO has developed a business case and a communication plan for IT governance, and needs to secure the support and commitment of the

key decision-makers and influencers6. Developing an IT balanced scorecard to monitor and track IT performance is a step that occurs after the new CIO has implemented and executed the IT governance framework, and needs to measure and report on the outcomes and benefits of IT governance7.

Reference: 1: Corporate governance of information technology - Wikipedia8 2: What is Business Value? Definition & Examples - Talend 3: How to Create an Effective IT Governance Framework | Smartsheet 4: 7 Rules for Demonstrating the Business Value of IT - Gartner 5: The internal process perspective within the Balanced Scorecard 6: Here's What You Need in Your Whistleblower Policy (and Why) - Case IQ 7: The Balanced Scorecard Customer Perspective : What is Enterprise Architecture? | Gartner

Question: 470

An enterprise has launched a critical new IT initiative that is expected to produce substantial value. Which of the following would BEST facilitate the reporting of benefits realized by the IT investment to the board?

A. Balanced scorecard
B. Milestone chart
C. Performance management
D. Critical risk and issue walk through

Answer: A

Explanation:

A balanced scorecard is a tool that helps to measure and communicate the value of IT initiatives to the board of directors. It aligns IT objectives with business goals, tracks performance indicators, and shows the contribution of IT to the enterprise value. A balanced scorecard can also help to identify gaps and areas for improvement in IT governance. Reference := CGEIT Review Manual, 7th Edition, Chapter 3: Benefits Realization, Section 3.3: Value Delivery Frameworks and Mechanisms, pp. 103105.

Question: 471

The MOST appropriate method for evaluating the capability of IT governance is through the use of:

A. a maturity assessment.
B. benchmarking.
C. a cost-benefit analysis.
D. a risk assessment.

Answer: A

Explanation:

A maturity assessment is the most appropriate method for evaluating the capability of IT governance because it helps to measure the current state of IT governance processes, identify gaps and areas for improvement, and align IT goals with business objectives. A maturity assessment can also provide a roadmap for achieving higher levels of IT governance maturity and performance. A maturity assessment can use various frameworks and models, such as the Gartner IT Score for CIOs1, the Forrester DEX Maturity Model2, the Capability Maturity Model3, or the Data Governance Maturity Model4. Reference := CGEIT Review Manual, 7th Edition, Chapter 1: Framework for the
Governance of Enterprise IT, Section 1.4: GEIT Implementation Approaches, pp. 23-24.

Question: 472

When a shortfall of IT resources is identified, the FIRST course of action is to;

A. perform a business impact analysis (BIA).
B. reallocate the budget to close the gap in resources.
C. reduce business requirements.
D. negotiate best pricing for contracted resources.

Answer: A

Explanation:

Performing a business impact analysis (BIA) is the first course of action when a shortfall of IT resources is identified because it helps to assess the potential impact of the resource gap on thebusiness processes, objectives, and goals. A BIA can also help to prioritize the criticality of the IT resources, identify the minimum acceptable levels of service, and determine the recovery strategies and resource requirements. A BIA can provide a basis for making informed decisions on how to allocate the available IT resources or acquire additional resources to close the gap.

Reference:

According to ISACA's CGEIT Review Manual 2021, one of the key activities for ensuring effective IT resource management is to "perform a business impact analysis (BIA) to identify and prioritize critical IT resources."1

According to ISACA's COBIT 2019 Framework, one of the governance objectives for managing IT resources is to "ensure that a BIA is performed to determine the required level of availability, continuity and security of IT services and data."2

According to ISACA's Business Continuity Management guide, one of the steps for developing a business continuity plan is to "conduct a BIA to identify the critical business processes and IT resources that support them."3

Question: 473

Which of the following is the BEST way to address the risk associated with new IT investments?

A. Develop security best practices to protect applications.
B. Integrate security requirements at the beginning of projects
C. Establish an enterprise-wide incident response process.
D. Implement an enterprise-wide security awareness program.

Answer: B

Explanation:

The best way to address the risk associated with new IT investments is to integrate security requirements at the beginning of projects. This means that security is considered as a key factor in the planning, design, development and testing phases of IT projects. By doing so, organizations can ensure that security is built into the IT solutions, rather than added as an afterthought. This can help to prevent or reduce security vulnerabilities, breaches, incidents and costs. Integrating security requirements at the beginning of projects is also consistent with the IT risk management frameworks that recommend a proactive and preventive approach to IT risk management12. Reference := Proactive IT Risk Management in an Era of Emerging Technologies, IT

Risk Management Process & Frameworks

Question: 474

Which of the following BEST enables an enterprise to achieve the benefits of implementing new Internet of Things (IoT) technology?

A. IT project charter
B. Change management
C. Emerging technology roadmap
D. Enterprise architecture (EA)

Answer: D

Explanation:

Enterprise architecture (EA) is the best way to enable an enterprise to achieve the benefits of implementing new Internet of Things (IoT) technology because it provides a holistic view of the current and desired state of the enterprise, including its business processes, information systems, data, applications, infrastructure, and security. EA helps to align the enterprise's vision, strategy, and goals with its IT capabilities and resources. EA also helps to identify the gaps, risks, and opportunities for improvement in the existing IT environment and to design and implement the optimal IT solutions that can support the business needs and objectives. EA can help to ensure that the new IoT technology is integrated seamlessly with the existing IT systems and that it delivers value to the stakeholders and customers. EA can also help to monitor and evaluate the performance and outcomes of the IoT technology and to ensure its compliance with the relevant standards, policies, and regulations12. Reference := Enterprise Architecture: A Framework for Driving Business Value from IoT,

Question: 475

A CIO was notified that a new employee was observed wearing a headset with an optical lens at the organization's data center. The individual was entering voice commands into the device. When approached, the employee explained the device is a new personal technology serving as a handsfree version of a smart phone. The CIO is concerned with potential security vulnerabilities of allowing such devices, and whether they should be banned from the facility. What should be the NEXT course of action in response to the ClO's concern?

A. Define a risk mitigation strategy.
B. Update the acceptable use policy.
C. Research competitor usage of similar devices.
D. Assess the risk associated with the device.

Answer: D

Explanation:

The next course of action in response to the CIO's concern is to assess the risk associated with the device. This means that the CIO should evaluate the potential impact and likelihood of security threats posed by the device, such as data leakage, unauthorized access, malware infection, or privacy violation. The CIO should also consider the benefits and drawbacks of allowing or banning such devices, such as productivity, innovation, user satisfaction, or compliance. A risk assessment can help the CIO to make an informed decision based on facts and evidence, rather than assumptions or
emotions. A risk assessment can also provide a basis for defining a risk mitigation strategy, updating the acceptable use policy, or researchingcompetitor usage of similar devices. Reference := 10 security risks of wearables | CSO Online, Wearable Devices are on the Rise, Presenting New Security Risks, Common privacy and security vulnerabilities in wearable devices, Wearables Device Data Security & Protection | Voler Systems

Question: 476

Which of the following is the BEST way for a CIO to ensure that the work of IT employees is aligned with approved IT directives?

A. Mandate technical training related to the IT objectives.
B. Have business leaders present their departments' objectives.
C. Include relevant IT goals in individual performance objectives.
D. Request a progress review of IT objectives by internal audit.

Answer: C

Explanation:

The best way for a CIO to ensure that the work of IT employees is aligned with approved IT directives is to include relevant IT goals in individual performance objectives. This means that the CIO should communicate the IT vision, mission, strategy and objectives to the IT staff and link them to their personal and professional development plans. By doing so, the CIO can motivate the IT employees to work toward the desired outcomes, monitor their progress and performance, provide feedback and recognition, and address any issues or gaps. Including relevant IT goals in individual performance objectives can also help to align the IT employees with the business needs and expectations, foster a culture of accountability and collaboration, and improve the quality and value of IT services12. Reference := How to Align Employee Performance With Organizational Goals, The

Importance And Challenges Of Employee Alignment

Question: 477

Which of the following would be MOST useful in developing IT strategic plans aligned with technological needs?

A. Business impact analysis (BIA)
B. Business case
C. Enterprise architecture (EA)
D. Benchmark analysis

Answer: C

Explanation:

Enterprise architecture (EA) is the most useful in developing IT strategic plans aligned with technological needs because it provides a holistic view of the current and desired state of the organization, including its business processes, information systems, data, applications, infrastructure, and security. EA helps to align the organization's vision, strategy, and goals with its IT capabilities and resources. EA also helps to identify the gaps, risks, and opportunities for improvement in the existing IT environment and to design and implement the optimal IT solutions that can support the business needs and objectives. EA can help to ensure that the IT strategic plans are consistent, coherent, and feasible12.

A business impact analysis (BIA) is a tool that helps to assess the potential impact of a disruption or change on the business objectives, processes, and functions. A BIA can help to prioritize the criticality of the IT resources and determine the acceptable level of risk and recovery time. A BIA can provide a basis for deciding how to allocate the budget, reduce the requirements, or contract external resources3. However, a BIA is not sufficient for developing IT strategic plans aligned with technological needs because it does not provide a comprehensive view of the current and future IT architecture and its alignment with the business strategy.

A business case is a document that describes the rationale and justification for initiating a project or investment. A business case can help to evaluate the costs, benefits, risks, and alternatives of different IT options and to communicate the value proposition to the stakeholders4. However, a business case is not enough for developing IT strategic plans aligned with technological needs because it does not provide a holistic view of the current and future IT architecture and its alignment with the business strategy.

A benchmark analysis is a process of comparing the performance, quality, or practices of an organization with those of its peers or competitors. A benchmark analysis can help to identify the best practices, standards, or trends in the industry and to measure the gap between the current and desired state of an organization. However, a benchmark analysis is not adequate for developing IT strategic plans aligned with technological needs because it does not provide a holistic view of the current and future IT architecture and its alignment with the business strategy.

Reference := Implement Agile IT Strategic Planning with Enterprise Architecture, The Benefits of Enterprise Architecture in Organizational Transformation, Business Impact Analysis, Business Case, [Benchmark Analysis]

Question: 478

Which of the following is the BEST indicator of the effectiveness of IT governance in an enterprise?

A. Value delivery
B. Resource utilization
C. Residual risk
D. Project delivery

Answer: A

Explanation:

Value delivery is the best indicator of the effectiveness of IT governance in an enterprise because it measures how well IT supports the business objectives and creates value for the stakeholders. The other options are important aspects of IT governance, but they are not as comprehensive as value delivery. Reference := ISACA, CGEIT Review Manual, 7th Edition, Chapter 1: Framework for the Governance of Enterprise IT, Section 1.2: Principles of IT Governance, p. 9.

Question: 479

An enterprise is assessing whether to utilize wearable technology. The enterprise has no prior experience with this technology and has asked the chief technology officer (CTO) to assess the impact to the enterprise. The CTO should FIRST:

A. understand the enterprise's risk tolerance.
B. create an IT risk scorecard.
C. prioritize wearable technology risk.

Answer: A

Explanation:

The CTO should first understand the enterprise's risk tolerance before assessing the impact of wearable technology. This will help the CTO to align the assessment with the enterprise's objectives, culture, and appetite for risk. The other options are important steps in the assessment process, but they are not the first ones. Creating an IT risk scorecard and prioritizing wearable technology risk require a clear understanding of the enterprise's risk tolerance, which is the basis for defining risk criteria and thresholds. Reference := ISACA, CGEIT Review Manual, 7th Edition, Chapter 2: Strategic Management, Section 2.3: Risk Optimization, p. 63-64.

Question: 480

An internal auditor conducts an assessment of a two-year-old IT risk management program. Which of the following findings should be of MOST concern to the CIO?

A. Organizational responsibility for IT risk management is not clearly defined.
B. None of the members of the IT risk management team have risk management-related certifications.
C. Only a few key risk indicators (KRIs) identified by the IT risk management team are being monitored and the rest will be on a phased schedule.
D. IT risk training records are not properly retained in accordance with established schedules

Answer: A

Explanation:

Organizational responsibility for IT risk management is a critical factor for the success of the program. Without clear roles and responsibilities, the program may lack accountability, coordination, communication and alignment with the business objectives. The other options are not as concerning as option A, because they do not affect the core of the program. Having risk management-related certifications is desirable, but not mandatory, for the IT risk management team. Monitoring only a few key risk indicators (KRIs) is acceptable, as long as they are relevant and meaningful for the program. Retaining IT risk training records is important, but not essential, for the program effectiveness. Reference := ISACA, CGEIT Review Manual, 7th Edition, Chapter 3: Benefits Realization, Section 3.2: IT Risk Management, p. 113-114.

Question: 481

The accountability for a business continuity program for business-critical systems is BEST assigned to the:

A. enterprise risk manager.
B. chief executive officer (CEO).
C. director of internal audit.
D. chief information officer (CIO).

Answer: D

Explanation:

The accountability for a business continuity program for business-critical systems is best assigned to the CIO, because the CIO is responsible for the IT strategy, operations, and resources that support the business objectives and continuity. The other options are not as suitable as the CIO, because they do not have the same level of authority, expertise, or involvement in the IT function. The enterprise risk manager oversees the overall risk management process, but does not have direct control over the IT resources and activities. The CEO is ultimately accountable for the entire organization, but delegates the responsibility for IT to the CIO. The director of internal audit provides assurance and consulting services on the effectiveness of governance, risk management, and control processes, but does not have operational responsibility for IT or business continuity. Reference := Business Continuity Program Roles & Responsibilities, Who Should Manage the Business Continuity Program?

Question: 482

An enterprise plans to migrate its applications and data to an external cloud environment. Which of the following should be the ClO's PRIMARY focus before the migration?

A. Reviewing the information governance framework
B. Selecting best-of-breed cloud offerings
C. Updates the enterprise architecture (EA) repository
D. Conducting IT staff training to manage cloud workloads

Answer: A

Explanation:

Reviewing the information governance framework should be the CIO's primary focus before the migration, because it will help the CIO to ensure that the enterprise's data and applications are secure, compliant, and aligned with the business objectives and policies in the cloud environment. The information governance framework defines the roles, responsibilities, processes, standards, and metrics for managing information assets across the enterprise. It also covers aspects such as data classification, data quality, data protection, data retention, data sovereignty, and data privacy. By reviewing the information governance framework, the CIO can identify the requirements, risks, and gaps that need to be addressed before moving to the cloud. The other options are not as important as reviewing the information governance framework, because they are either dependent on or secondary to it. Selecting best-of-breed cloud offerings is a tactical decision that should be based on the information governance framework and the enterprise architecture. Updating the enterprise architecture repository is a good practice, but not a primary focus before the migration. It can be done after the migration to reflect the changes in the IT landscape. Conducting IT staff training to manage cloud workloads is a necessary step, but not a primary focus before the migration. It can be done in parallel with or after the migration to ensure that the IT staff have the skills and knowledge to operate and optimize the cloud environment. Reference := Migration environment planning checklist, Practical Guide to Cloud Governance, Governance or compliance strategy

Question: 483

Which of the following is the MOST important consideration when integrating a new vendor with an enterprise resource planning (ERP) system?

A. IT senior management selects the vendor.
B. A vendor risk assessment is conducted
C. ERP data mapping is approved by the enterprise architect.
D. Procurement provides the terms of the contract.

Answer: B

Explanation:

A vendor risk assessment is the most important consideration when integrating a new vendor with an ERP system, because it helps to identify and evaluate the potential risks or hazards associated with the vendor's operations and products and their impact on the organization. A vendor risk assessment can cover aspects such as security, compliance, quality, reliability, performance, and contingency plans. By conducting a vendor risk assessment, the organization can mitigate the risks and ensure a smooth and secure integration with the ERP system. The other options are not as important as a vendor risk assessment, because they are either dependent on or secondary to it. IT senior management selects the vendor based on the results of the vendor risk assessment and other criteria. ERP data mapping is approved by the enterprise architect afterthe vendor risk assessment confirms that the vendor's data is compatible and consistent with the ERP system. Procurement provides the terms of the contract after the vendor risk assessment validates that the vendor meets the organizational standards and obligations. Reference := Guide to Vendor Risk Assessment, 10 Risk Assessment Factors for ERP System Integration Projects, Ensuring Vendor Compliance and Third- Party Risk Mitigation

Question: 484

Which of the following would provide the MOST useful information to measure the alignment of IT with the enterprise?

A. Balanced scorecard
B. Control self-assessment (CSA)
C. Gap analysis
D. Audit reports

Answer: A

Explanation:

A balanced scorecard is a strategic management tool that measures the alignment of IT with the enterprise by using four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard helps to translate the enterprise vision and strategy into IT objectives, measures, targets, and initiatives. It also helps to monitor and evaluate the IT performance and value delivery in relation to the enterprise goals and stakeholder expectations. A balanced scorecard provides a comprehensive and balanced view of the IT contribution to the enterprise success. The other options are not as useful as a balanced scorecard for measuring the alignment of IT with the enterprise, because they are either too narrow or too subjective. A control self-assessment (CSA) is a technique that involves the participation of staff in assessing the effectiveness of internal controls and risk management processes. A CSA can provide some insights into the IT alignment with the enterprise, but it is not a systematic or holistic approach. A gap analysis is a method that compares the current state and the desired state of a process or a system and identifies the gaps or discrepancies that need to be addressed. A gap analysis can help to improve the IT alignment with the

enterprise, but it is not a measurement tool. Audit reports are documents that present the findings and opinions of an independent auditor on the adequacy and compliance of an audited entity. Audit reports can provide some evidence of the IT alignment with the enterprise, but they are not a comprehensive or consistent measure. Reference := The art of measurement in enterprise and business architecture, Benchmarking strategic alignment of business and IT strategies, The Importance of Business & IT Alignment, 7 ways to effectively ensure IT-business alignment

Question: 485

Which of the following is MOST important for a data steward to verify when a system's data is edited by an automated tool to fix an incident?

A. The change has been requested by the business department and approved by the data owner.
B. The change is documented in preparation for future audits.
C. The change maintains consistency among databases and has no other impacts.
D. The change is a temporary fix for the incident, and the permanent solution is addressed by problem management.

Answer: C

Explanation:

The most important thing for a data steward to verify when a system's data is edited by an automated tool to fix an incident is that the change maintains consistency among databases and has no other impacts. Data consistency is a dimension of data quality that describes the data's uniformity as it moves across applications and networks and when it comes from multiple sources1. Data is considered consistent if two or more values in different locations are identical and do not conflict1. Data consistency is related to data integrity and data currency1. To ensure data consistency, some steps include data governance, automated data integration, and regular data audits and quality control checks1. If the automated tool changes the data in one database, but not in others, it can create inconsistencies and errors that affect the reliability and usability of the data. Similarly, if the automated tool changes the data in a way that affects other processes or systems that depend on the data, it can cause disruptions and failures that impact the business operations and performance. Therefore, the data steward should verify that the change is consistent and has no other impacts before approving it.

The other options are not as important as verifying the data consistency and impact of the change. Requesting and approving the change by the business department and the data owner is a good practice, but not a verification step. Documenting the change in preparation for future audits is a necessary step, but not a verification step. Addressing the permanent solution for the incident by problem management is a relevant step, but not a verification step. Reference := What is Data Quality - Definition, Dimensions … - Simplilearn

Question: 486

What is the BEST way for IT to achieve compliance with regulatory requirements?

A. Enforce IT policies and procedures.
B. Create an IT project portfolio.
C. Review an IT performance dashboard.
D. Report on IT audit findings and action plans.

Answer: A

Explanation:

The best way for IT to achieve compliance with regulatory requirements is to enforce IT policies and procedures

that align with the compliance standards and guidelines. IT policies andprocedures are the documents that define the roles, responsibilities, rules, and expectations for the IT function and its activities. They help to ensure that the IT systems and processes are secure, reliable, efficient, and consistent with the business objectives and legal obligations. By enforcing IT policies and procedures,
IT can demonstrate its compliance with regulatory requirements and avoid violations, penalties, or reputational damage. The other options are not as effective as enforcing IT policies and procedures for achieving compliance with regulatory requirements. Creating an IT project portfolio is a good practice for managing IT investments and resources, but it does not guarantee compliance with regulatory requirements. Reviewing an IT performance dashboard is a useful technique for monitoring and measuring IT performance and value delivery, but it does not ensure compliance with regulatory requirements. Reporting on IT audit findings and action plans is a necessary step for improving IT governance and control processes, but it does not achieve compliance with regulatory requirements. Reference := What is IT Compliance? - Checklist, Guidelines & More | Proofpoint US, 6 Common IT Compliance Standards (A Guide to the Basics), Here's Why Regulatory Compliance is Important - Reciprocity

Question: 487

Which of the following is the PRIMARY role of the governance function in enabling an enterprise to achieve its business objectives?

A. Determining risk thresholds that the enterprise can sustain
B. Preparing business continuity and resiliency plans
C. Providing a means to effectively manage stakeholders
D. Monitoring strategic plans to reach the desired target state

Answer: C

Explanation:

The primary role of the governance function in enabling an enterprise to achieve its business objectives is to provide a means to effectively manage stakeholders. Stakeholders are the individuals or groups that have an interest or stake in the enterprise's activities, outcomes, and performance. They include shareholders, customers, employees, suppliers, regulators, and society at large. Effective stakeholder management involves identifying, engaging, communicating, and satisfying the needs and expectations of the stakeholders in a transparent and ethical manner. By providing a means to effectively manage stakeholders, the governance function can help the enterprise to align its vision, mission, strategy, and values with the stakeholder interests, foster trust and collaboration among the stakeholder groups, balance the economic and social goals and the individual and communal goals of the enterprise, and enhance the reputation and legitimacy of the enterprise in the market and society.
The other options are not as primary as providing a means to effectively manage stakeholders for the governance function. Determining risk thresholds that the enterprise can sustain is animportant aspect of the governance function, but it is not the primary role. Risk thresholds are the levels of risk exposure that the enterprise is willing to accept or tolerate in pursuit of its business objectives. They are derived from the enterprise's risk appetite and risk tolerance statements, which reflect the enterprise's culture, values, and strategy. The governance function can help to define, communicate, and monitor the risk thresholds that the enterprise can sustain, but this is not its primary role. Preparing business continuity and resiliency plans is a vital responsibility of the management function, not the governance function. Business continuity and resiliency plans are the documents that outline the processes and procedures for ensuring the continuity of critical business functions and operations in the event of a disruption or crisis. They also describe how the enterprise can recover from the disruption or crisis and resume normal operations as soon as possible. The governance function can oversee and approve the business continuity and resiliency plans prepared by the management function, but this is not its primary role. Monitoring strategic plans to reach the

desired target state is a key activity of both the governance function and the management function, but it is not their primary role. Strategic plans are the documents that define the long-term goals and objectives of the enterprise and how they will be achieved. They also specify the resources, actions, measures, and timelines for implementing the strategy. The governance function can set the direction and scope of the strategic plans, while the management function can execute and report on them. Both functions can monitor the progress and performance of the strategic plans to reach the desired target state, but this is not their primary role. Reference := The five functions of governance – Project Manager, What is a Governance Structure? - ESG | The Report, Develop an effective governance structure | Australian Public Service …

Question: 488

Which of the following would be MOST helpful to review when determining how to allocate IT resources during a resource shortage?

A. IT strategic plan
B. IT skills inventory
C. IT organizational structure
D. IT skill development plan

Answer: B

Explanation:

An IT skills inventory is a list of the skills, competencies, and qualifications of the IT staff in an organization. It can help to identify the current and potential capabilities of the IT workforce, as well as the gaps and needs for improvement. An IT skills inventory would be most helpful to review when determining how to allocate IT resources during a resource shortage, because it canhelp to match the right people with the right tasks, optimize the utilization and productivity of the existing IT staff, and prioritize the critical and urgent IT activities. The other options are not as helpful as an IT skills inventory for allocating IT resources during a resource shortage. An IT strategic plan is a document that defines the vision, mission, goals, and objectives of the IT function and how they align with the business strategy. It can help to guide the direction and scope of the IT activities and investments, but it does not provide detailed information on the availability and suitability of the IT resources. An IT organizational structure is a diagram that shows the hierarchy, roles, and responsibilities of the IT staff in an organization. It can help to clarify the reporting lines and communication channels of the IT function, but it does not reflect the skills and competencies of the IT staff. An IT skill development plan is a document that outlines the learning and training opportunities for the IT staff to enhance their skills and competencies. It can help to improve the performance and career progression of the IT staff, but it does not address the immediate needs and challenges of allocating IT resources during a resource shortage. Reference := What is an IT Skills Inventory?, How to Conduct an Effective Skills Gap Analysis, Resource allocation 101: How to manage your team's resources | Planio

Question: 489

Which of the following is the PRIMARY benefit to an enterprise when risk management is practiced effectively throughout the organization?

A. Decisions are made with an awareness of probability and impact.
B. IT objectives and goals are aligned to business objectives and goals.
C. Business opportunity losses are minimized.
D. Innovative strategic initiatives are encouraged.

Answer: A

Explanation:

Risk management is the process of identifying, analyzing, evaluating, and treating the uncertainties that may affect the achievement of objectives. Risk management helps to ensure that decisions are made with an awareness of probability and impact, which means that the likelihood and consequences of potential events are considered and weighed against the benefits and costs of the actions. This can help to optimize the risk-reward balance, enhance the quality and consistency of decision-making, and support the achievement of desired outcomes. Reference:

CGEIT Review Manual 2021, Chapter 2: IT Risk Management, Section 2.1: Risk Management Overview, page 551

CGEIT Review Questions, Answers & Explanations Manual 2021, Question 1, page 152

The Benefits of Risk Management - PMI3

Question: 490

Which of the following is the BEST way to manage the risk associated with outsourcing critical IT services?

A. Ensure vendors hold information security certifications.
B. Define controls within service level agreements (SLAs).
C. Conduct quarterly performance reviews.
D. Ensure exit clauses are added to the contract.

Answer: B

Explanation:

This is because SLAs are contractual agreements that specify the expectations, responsibilities, and performance standards for both the service provider and the customer. SLAs can help to define controls that mitigate the risks of outsourcing, such as data security, quality, availability, reliability, compliance, and contingency. SLAs can also help to monitor and measure the performance and value of the outsourced services, as well as to establish mechanisms for reporting, escalation, and resolution of any issues or disputes.

Some of the sources that support this answer are:

1: This source provides a comprehensive guide on how to create a social media governance plan that covers the key elements of a social media policy, compliance management, security and risk mitigation, decision-making and approval workflow, and crisis management. It mentions that SLAs are one of the tools that can help to manage the risks of outsourcing social media activities to third parties.

2: This source discusses the gaps, risks, and opportunities of social media governance in the context of Australian public communication. It suggests that SLAs are one of the best practices for developing and implementing a social media strategy that aligns with the organizational goals and values, as well as the legal and ethical obligations.

3: This source explores the benefits and challenges of outsourcing IT services in the public sector. It emphasizes the importance of SLAs for defining the scope, quality, and cost of the outsourced services, as well as for managing the performance and accountability of the service providers.

4: This source presents a framework for managing IT outsourcing risks based on ISO 31000. It recommends that SLAs should include risk-related clauses that specify the roles and responsibilities of both parties, the risk identification and assessment methods, the risk response and treatment options, and the risk monitoring and reporting mechanisms.

Question: 491

Which of the following should be the PRIMARY consideration when implementing an emerging technology with unclear regulatory and compliance requirements?

A. Enterprise strategic plan
B. Enterprise architecture (EA) alignment
C. Enterprise risk appetite
D. Business impact analysis (BIA) results

Answer: C

Explanation:

This is because enterprise risk appetite is the amount and type of risk that an organization is willing and able to accept in pursuit of its objectives. It reflects the organization's risk culture, strategy, and values. When implementing an emerging technology with unclear regulatory and compliance requirements, the organization should consider its risk appetite and tolerance, as well as the potential benefits, costs, and impacts of the technology. The organization should also assess the likelihood and severity of the regulatory and compliance risks, and implement appropriate controls and mitigation measures to manage them within acceptable levels.

Some of the sources that support this answer are:

1: This source provides a comprehensive guide on how to navigate the hype and risk of emerging technologies. It suggests that organizations should define their risk appetite and tolerance for adopting emerging technologies, and conduct a balanced risk and benefit assessment before making any decisions.

2: This source discusses the challenges and best practices for mitigating emerging technology risk. It recommends that organizations should align their emerging technology strategy with their enterprise risk appetite, and establish a governance framework that covers the identification, evaluation, response, and monitoring of emerging technology risks.

3: This source defines enterprise risk appetite and explains its importance for effective risk management. It also provides some guidance on how to develop, communicate, and monitor enterprise risk appetite statements.

Question: 492

To help ensure the IT portfolio provides maximum value to an organization, IT projects are BEST prioritized based on:

cost-benefit analysis results.

alignment with business strategy.

A. recommendation Of business owners.
B. alignment with IT architecture.

Answer: B

Explanation:

This is because alignment with business strategy means that IT projects are selected and executed in a way that

supports the organization's vision, mission, goals, and objectives. Alignment with business strategy can help to ensure that IT projects deliver value to the organization and its stakeholders, as well as to optimize the use of IT resources and capabilities. Alignment with business strategy can also help to avoid or minimize conflicts, gaps, or redundancies among IT projects, as well as to facilitate communication and collaboration among IT and business units.

Some of the sources that support this answer are:

1: This source provides a comprehensive guide on how to optimize IT project intake, approval, and prioritization. It suggests that one of the steps to redesign the governance framework is to conduct a portfolio review to assess the benefits realization of IT investments and ensure that they are aligned with the business strategy and deliver value.

2: This source discusses how to prioritize IT tasks and projects, and provides some expert tips and a downloadable template. It advises that one of the criteria for prioritizing IT projects is strategic alignment, which means that the project supports the organization's strategic goals and objectives.

3: This source describes the process of how to use the Technology Governance Framework to determine if a proposal requires approval from a formal IT governance body, then how a submitted proposal would proceed on its path to acceptance. It states that one of the factors that influence the prioritization of proposals is alignment with strategic direction, which means that the proposal supports the organization's vision, mission, values, and goals.

Question: 493

When establishing a methodology for business cases, it would be MOST beneficial for an enterprise to include procedures for:

A. updating the business case throughout its life cycle.
B. addressing required changes outside the business case.
C. identifying metrics post-implementation to measure project success.
D. entering the business case into the enterprise architecture (EA).

Answer: A

Explanation:

This is because a business case is a document that provides the justification and rationale for initiating, continuing, or terminating a project or program. It describes the business problem or opportunity, the objectives and benefits, the costs and risks, the alternatives and assumptions, and the expected outcomes and value of the proposed solution. A business case is not a static document, but rather a dynamic one that should be updated throughout the life cycle of the project or program, as new information, changes, and feedback emerge. Updating the business case throughout its life cycle can help to ensure that the project or program remains aligned with the business strategy and goals, as well as to monitor and evaluate its performance and value delivery.

Some of the sources that support this answer are:

1: This source provides a comprehensive guide on how to write a business case, including its purpose, structure, content, and format. It also explains why it is important to update the business case throughout the project or program life cycle, as it can help to track progress, measure benefits, manage risks, and communicate results.

2: This source discusses the benefits and challenges of updating the business case during the project or program execution. It suggests that updating the business case can help to validate assumptions, verify feasibility, adjust scope, and justify changes. It also provides some tips and best practices for updating the

business case effectively and efficiently.

3: This source defines what a business case is and how it can be used to support IT governance and decision-making. It states that a business case should be updated regularly throughout the project or program life cycle, as it can help to ensure alignment with the enterprise architecture (EA), assess risks and opportunities, and demonstrate value realization.

Question: 494

Which of the following is the GREATEST expected strategic organizational benefit from the standardization of technical platforms?

A. Reduces IT operational training costs
B. Reduces response time
C. Optimizes infrastructure investments
D. Meets regulatory compliance requirements

Answer: C

Explanation:

Standardization of technical platforms can help optimize infrastructure investments by reducing complexity, increasing interoperability, and enabling economies of scale.

Reference:

According to the CGEIT Review Manual 2022, one of the benefits of standardization is that it “optimizes infrastructure investments by reducing complexity and increasing interoperability and scalability.”

According to the Oracle article on the EA Roadmap to Rationalize, Standardize, and Consolidate IT Assets, standardized technology "yields measurable cost savings through reduced software licenses and the elimination of redundant systems and skill sets."1

Question: 495

To measure the value of IT-enabled investments, an enterprise needs to identify its drivers as defined by its:

A. technology strategy.
B. value statements.
C. service level agreements (SLAs).
D. business strategy.

Answer: D

Explanation:

To measure the value of IT-enabled investments, an enterprise needs to identify its drivers as defined by its business strategy. The business strategy is the document that defines the vision, mission, goals, and objectives of the enterprise and how they will be achieved. It also specifies the value proposition, competitive advantage, and target market of the enterprise. The drivers ofvalue are the factors that influence or determine the value creation and delivery of the enterprise. They can include aspects such as customer satisfaction, revenue growth, cost reduction, innovation, quality, and efficiency. By identifying its drivers as defined by its business strategy, the enterprise can align its IT-enabled investments with its strategic

priorities and expectations. It can also establish the criteria, metrics, and indicators for measuring and evaluating the value of IT-enabled investments in terms of their contribution to the business outcomes and performance.

Question: 496

The BEST way for a CIO to justify maintaining and supporting social media platforms is by demonstrating:

A. how social media technology fits into the IT investment management process.
B. that service level agreements (SLAs) for social media technologies have been met.
C. the IT performance Of social media technologies.
D. the value derived from investment in social media technologies.

Answer: D

Explanation:

The best way for a CIO to justify maintaining and supporting social media platforms is by demonstrating the value derived from investment in social media technologies. Social media platforms are not just tools for communication and entertainment, but also strategic assets that can create and deliver value to the organization and its stakeholders. Some of the potential benefits of social media platforms are:
Enhancing customer engagement, loyalty, and satisfaction by providing timely, personalized, and interactive content and feedback
Increasing brand awareness, reputation, and trust by showcasing the organization's values, achievements, and social responsibility
Improving innovation and collaboration by facilitating the exchange of ideas, knowledge, and feedback among employees, customers, partners, and experts
Supporting decision making and problem solving by providing access to relevant data, insights, and analytics
Reducing costs and increasing efficiency by streamlining processes, automating tasks, and optimizing resources

Question: 497

Which of the following should a new CIO do FIRST to set the strategic direction for IT?

A. Develop well-defined business cases that include strategic outcomes.
B. Remap stakeholder analysis and desired expectations.
C. Review existing enterprise strategic objectives.
D. Redesign detailed RACI charts of the IT function.

Answer: C

Explanation:

The first thing that a new CIO should do to set the strategic direction for IT is to review the existing enterprise strategic objectives. The enterprise strategic objectives are the high-level goals and priorities that guide the organization's vision, mission, and value creation. The CIO should understand the current state and desired state of the enterprise, as well as the opportunities, challenges, and risks that it faces. The CIO should also assess how IT supports and enables the enterprise strategic objectives, and identify any gaps, issues, or areas

for improvement.

The other options are not the first thing that a new CIO should do to set the strategic direction for IT. Developing well-defined business cases that include strategic outcomes is part of the IT investment management process, which involves selecting, prioritizing, approving, and funding IT projects and initiatives that deliver value to the enterprise. Remapping stakeholder analysis and desired expectations is part of the stakeholder engagement process, which involves identifying, communicating, and managing the needs and expectations of the internal and external stakeholders of IT. Redesigning detailed RACI charts of the IT function is part of the IT organizational design process, which involves defining and assigning the roles, responsibilities, authorities, and accountabilities of the IT staff and units.

Reference:

According to the CGEIT Review Manual 2022, "The first step in developing an IT strategy is to understand the enterprise strategy. This involves analyzing the enterprise vision, mission, goals, objectives, value drivers, critical success factors, and SWOT (strengths, weaknesses, opportunities and threats)."1

According to the ISACA article on How to Develop an Effective IT Strategy2, “The first step in developing an effective IT strategy is to understand your organization’s business strategy. This will help you align your IT goals with your business goals and ensure that your IT investments support your business objectives.”

According to the CIO article on How to create an effective IT strategy3, “The first step in creating an effective IT strategy is to understand what your business is trying to achieve. Thismeans reviewing your business strategy and identifying the key drivers of value and competitive advantage for your organization.”

Question: 498

When an enterprise is evaluating potential IT service vendors, which of the following BEST enables a clear understanding of the vendor's capabilities that will be critical to the enterprise's strategy?

Due diligence process

A. Independent audit results
B. Historical service level agreements (SLAs)
C. Benchmarking analysis results

Answer: A

Explanation:

A due diligence process is the best way to enable a clear understanding of the vendor’s capabilities that will be critical to the enterprise’s strategy. A due diligence process is a systematic and comprehensive investigation and evaluation of the vendor’s background, reputation, performance, quality, reliability, security, compliance, and suitability for the enterprise’s needs and expectations. A due diligence process can help the enterprise:

Verify the vendor’s claims and credentials, and validate the vendor’s references and testimonials Assess the vendor’s financial stability, legal status, and ethical standards

Identify the vendor’s strengths, weaknesses, opportunities, and threats

Compare the vendor’s offerings, capabilities, and prices with other vendors and market benchmarks Determine the risks and benefits of engaging with the vendor, and the mitigation and contingency plans

Negotiate the terms and conditions of the contract, service level agreement (SLA), and key performance indicators (KPIs)

Reference:

According to the CGEIT Review Manual 2022, "Due diligence is a comprehensive appraisal of a business undertaken by a prospective buyer or partner to establish its assets and liabilities and evaluate its commercial potential."1

According to the ISACA article on Third-Party Vendor Selection: If Done Right, It's a Win-Win2, "Once you have identified which processes can be outsourced as well as their inherent risks, you can begin performing due diligence on potential vendors. The level of due diligence should be tailored to the significance of the relationship as well as the potential risks it poses."

According to the Gartner article on How to Evaluate Technology Vendors in 4 Rigorous Steps1, "Evaluating vendors requires detailed objectives, criteria, prioritization and monitoring. Here's help. When it comes to choosing a vendor, enterprise tech buyer teams can easily become bogged down in the details and documentation provided by sales teams."

Question: 499

An enterprise has an ongoing issue of corporate applications not delivering the expected benefits due to missing key functionality. As a result, many groups are using spreadsheets and databases instead of approved enterprise applications to store and manipulate information. Which of the following will BEST improve the success rate of future IT initiatives?

A. Engage the business user community in acceptance testing Of acquired applications.
B. Engage stakeholders to identify and validate business requirements.
C. Establish a process for risk and value management.
D. Prohibit the use of non-approved alternate software solutions.

Answer: B

Explanation:

Engaging stakeholders to identify and validate business requirements is the best way to improve the success rate of future IT initiatives. Stakeholders are the individuals or groups who have an interest or influence in the IT initiatives, such as business users, customers, managers, sponsors, etc.

Engaging stakeholders can help:

Understand the needs, expectations, and priorities of the stakeholders, and ensure that they are aligned with the business objectives and strategy

Define and document the business requirements that specify what the IT initiatives should deliver in terms of functionality, quality, performance, and value

Validate and verify that the business requirements are clear, complete, consistent, feasible, and testable

Communicate and manage any changes or issues that may affect the business requirements or the IT initiatives

Engaging stakeholders to identify and validate business requirements can help avoid missing key functionality in the corporate applications, and ensure that they meet the stakeholder's needs and expectations. This can also reduce the reliance on spreadsheets and databases as alternative software solutions, and increase the user satisfaction and adoption of the enterprise applications. The other options are not the best way to improve the success rate of future IT initiatives. Engaging the business user community in acceptance testing of acquired applications is a good practice, but it is not sufficient to ensure that the applications have the key functionality that meets the business requirements. Acceptance testing is done at the end of the IT initiative lifecycle, after the applications have been developed or acquired. If the business requirements were not properly identified and validated at the beginning of the IT initiative lifecycle, acceptance testing may reveal significant gaps or defects that may be costly or difficult to fix. Establishing a process for risk and value management is a useful

technique, but it does not directly address the issue of missing key functionality in the corporate applications.
Risk and value management involves identifying, assessing, prioritizing, and treating the risks and benefits associated with IT initiatives. However, without clear and valid business requirements, risk and value management may not be effective or accurate. Prohibiting the use of non-approved alternate software solutions is a restrictive measure, but it does not solve the problem of missing key functionality in the corporate applications.
Prohibiting the use of spreadsheets and databases may force the users to use the enterprise applications, but it may also create dissatisfaction, frustration, or resistance among them. Moreover, it may prevent them from performing their tasks efficiently or effectively if the enterprise applications do not meet their needs.
For more information on engaging stakeholders to identify and validate business requirements, you can refer to these web sources:
Stakeholder Engagement - ISACA Business Requirements - ISACA Requirements Validation - ISACA

Question: 500

Which of the following is necessary for effective risk management in IT governance?

A. Risk evaluation is embedded in the management processes.
B. IT risk management is separate from enterprise risk management (ERM).
C. Local managers are solely responsible for risk evaluation.
D. Risk management strategy is approved by the audit committee.

Answer: A

Explanation:

Effective risk management in IT governance requires that risk evaluation is embedded in the management processes of the organization. This means that risk evaluation is not a separate or isolated activity, but rather an integral part of the planning, execution, monitoring, and reporting of IT activities and initiatives. Embedding risk evaluation in the management processes can help: Identify and assess the potential threats and opportunities that may affect the achievement of IT and business objectives
Align the IT risk appetite and tolerance with the enterprise risk appetite and tolerance
Prioritize and allocate the resources and actions to address the risks based on their impact and likelihood
Monitor and report the risk performance and outcomes in relation to the IT value drivers and benefits
Embed the risk culture and awareness across the organization
Reference:
According to the CGEIT Review Manual 2022, "Risk evaluation should be embedded in management processes. Risk evaluation should be performed as part of planning, executing, monitoring and reporting activities."1
According to the ISACA article on Risk Management: A Driver for Value Creation2, “Risk management should be embedded into all business processes. It should be part of strategic planning, project management, change management, performance management, etc.”
According to the NIST article on Staging Cybersecurity Risks for Enterprise Risk Management and Governance3, “Embedding cybersecurity risk management into enterprise risk management (ERM) processes can help organizations better understand their cybersecurity risks, prioritize them based on their potential impact on business objectives, and allocate resources accordingly.”

Question: 501

When identifying improvements focused on the information asset life cycle, which of the following is

CRITICAL for enabling data interoperability?

A. Standardization
B. Replication
C. Segregation
D. Sanitization

Answer: A

Explanation:

Standardization is the process of establishing and applying common rules, formats, definitions, and methods for data collection, storage, processing, and exchange. Standardization is critical for enabling data interoperability, which is the ability of data to be shared and used across different systems, platforms, applications, and organizations. Standardization can help improve data interoperability by:
Enhancing the quality, consistency, and accuracy of data
Reducing the complexity and ambiguity of data
Increasing the compatibility and comparability of data
Facilitating the integration and analysis of data
Promoting the reuse and sharing of data
Reference:
According to the CGEIT Review Manual 2022, "Standardization is the process of developing and implementing technical standards. The goals of standardization can be to help with independence of single suppliers (commoditization), compatibility, interoperability, safety, repeatability or quality."1 According to the UN Statistics Wiki on Data Interoperability Guide2, “Standardization is a key enabler for interoperability. It allows for a common understanding of data elements across different systems and domains.”
According to the ISO/IEC 38500:2015 standard on Information technology — Governance of IT for the organization3, “Standardization can improve interoperability between systems within an organization or between organizations.”

Question: 502

A CEO realizes the need to implement IT governance to support the strategic alignment of business and IT goals. Which of the following would BEST enable this initiative?

A. A RACI chart
B. An increased IT budget
C. Well-trained IT staff
D. Effective culture change

Answer: D

Explanation:

Effective culture change is the process of transforming the values, beliefs, behaviors, and norms of the organization and its stakeholders to support the strategic alignment of business and IT goals. Effective culture change can enable the implementation of IT governance by:
Creating a shared vision and understanding of the purpose, benefits, and expectations of IT governance
Engaging and empowering the stakeholders to participate and collaborate in IT governance activities and

decisions

Fostering a culture of trust, transparency, accountability, and responsibility for IT governance outcomes

Encouraging a culture of innovation, learning, and improvement for IT governance processes and practices

Aligning the incentives and rewards with the IT governance objectives and performance Reference:

According to the CGEIT Review Manual 2022, "Culture is a key enabler for effective IT governance. Culture influences how people behave, communicate, collaborate, and make decisions. Culture also affects how people perceive, value, and use IT. Therefore, culture change is often necessary to implement IT governance successfully."1

According to the ISACA article on Culture Change: A Critical Success Factor for Effective IT Governance2, "Culture change is not an easy task; it requires strong leadership, clear communication, stakeholder involvement, and continuous monitoring and feedback. However, culture change can also bring significant benefits for IT governance, such as improved alignment, engagement, performance, and value creation."

According to the CIO article on How to create a culture of innovation in IT3, "Creating a culture of innovation in IT requires more than hiring talented people and acquiring the latest technologies. It also requires a shift in mindset, behavior, and structure that fosters creativity, collaboration, experimentation, and learning."

Question: 503

An enterprise has a centralized IT function but also allows business units to have their own technology operations, resulting in duplicate technologies and conflicting priorities. Which of the following should be done FIRST to reduce the complexity of the IT landscape?

Promote automation tools used by the business units.

A. Conduct strategic planning with business units.
B. Migrate all in-house systems to an external cloud environment.
C. Standardize technology architecture on common products.

Answer: B

Explanation:

The first thing that should be done to reduce the complexity of the IT landscape is to conduct strategic planning with business units. Strategic planning is the process of defining the vision, mission, goals, and objectives of the enterprise and how they will be achieved. It also involves aligning the IT strategy with the business strategy and ensuring that they support each other. By conducting strategic planning with business units, the enterprise can identify and prioritize the IT needs and expectations of each business unit, as well as the commonalities and synergies among them. This can help to reduce the complexity of the IT landscape by eliminating duplicate technologies, resolving conflicting priorities, and creating a coherent and consistent IT architecture that meets the business requirements and delivers value. The other options are not as effective as conducting strategic planning with business units for reducing the complexity of the IT landscape. Promoting automation tools used by the business units may improve efficiency and productivity, but it does not address the underlying issues of duplication and conflict. Migrating all in-house systems to an external cloud environment may reduce costs and increase scalability, but it does not ensure alignment and integration of IT systems across business units. Standardizing technology architecture on common products may simplify IT operations and maintenance, but it does not consider the specific needs and preferences of each business unit.

Question: 504

Of the following, who is responsible for the achievement of IT strategic objectives?

A. IT steering committee
B. Business process owners
C. Chief information officer (CIO)
D. Board of directors

Answer: C

Explanation:

The chief information officer (CIO) is the senior executive who is responsible for the achievement of IT strategic objectives. The IT strategic objectives are the high-level goals and priorities that guide the IT vision, mission, and value creation for the organization. The CIO is responsible for:

Developing and communicating the IT strategy and aligning it with the business strategy and objectives
Managing and delivering the IT solutions, services, and projects that support and enable the business needs, requirements, and value drivers
Leading and overseeing the IT functions, resources, and capabilities, and ensuring their quality, efficiency, and effectiveness
Monitoring and reporting the IT performance and outcomes, and ensuring their alignment with the IT strategic objectives and value drivers
Implementing and maintaining the IT governance framework, policies, standards, and practices The other options are not correct. The IT steering committee is a group of senior executives and stakeholders who provide guidance, direction, and oversight for the IT strategy and initiatives, but not responsible for their achievement. The business process owners are the individuals or groups who have an interest or influence in the business processes that are supported or enabled by IT, but not responsible for the achievement of IT strategic objectives. The board of directors is the highest governing body of the organization that sets the vision, mission, strategy, and objectives of the organization, as well as oversees its performance and value creation, but not responsible for the achievement of IT strategic objectives.

Reference:

According to the CGEIT Review Manual 20221, "The CIO is responsible for ensuring that IT strategic objectives are achieved. The CIO should develop an IT strategy that is aligned withenterprise strategy; manage IT resources to deliver value; monitor IT performance; implement IT governance; etc."

According to the CIO article on What is a CIO? Everything you need to know about the Chief Information Officer role2, "The chief information officer (CIO) oversees an organization's technology strategy, as well as the hardware, software and data that helps other departments do their jobs." According to the ISACA article on The Role of CIO in Enterprise Governance of Information Technology3, "The CIO plays a key role in EGIT by translating business strategy into IT strategy; managing IT resources; delivering IT solutions; measuring IT performance; ensuring compliance; etc."

Question: 505

An enterprise has decided to use third-party software for a business process which is hosted and supported by the same third party. The BEST way to provide quality of service oversight would be to establish a process:

A. for robust change management.

B. for periodic service provider audits.
C. for enterprise architecture (EA) updates.
D. to qualify service providers.

Answer: B

Explanation:

A periodic service provider audit is a process of conducting an independent and objective assessment of the service provider's performance, quality, compliance, and security in relation to the agreed service level agreement (SLA) and the enterprise's expectations and requirements. A periodic service provider audit can help provide quality of service oversight by:

Verifying and validating the service provider's claims and credentials, and ensuring that they meet the contractual obligations and standards

Identifying and evaluating the strengths, weaknesses, opportunities, and threats of the service provider's services, processes, and controls

Detecting and reporting any issues, gaps, or risks that may affect the quality of service delivery or the enterprise's objectives and value

Recommending and implementing corrective and preventive actions to address and resolve the issues, gaps, or risks

Monitoring and measuring the outcomes and effectiveness of the corrective and preventive actions, and ensuring their alignment with the SLA

Reference:

According to the CGEIT Review Manual 20221, "Service provider audits are a key mechanism for ensuring that service providers are meeting their contractual obligations and delivering value to the enterprise. Service provider audits should be conducted periodically or as needed to assess the performance, quality, compliance, and security of the service provider's services, processes, and controls."

According to the ISACA article on IT Outsourcing: Audit Considerations2, "IT outsourcing audit is a process of examining and evaluating the IT outsourcing arrangements between an enterprise and its service providers. IT outsourcing audit aims to provide assurance that the IT outsourcing arrangements are aligned with the enterprise's strategy, objectives, and risk appetite; that the service providers are delivering the expected services in accordance with the SLAs; that the service providers are complying with the applicable laws, regulations, and standards; and that the service providers are managing and mitigating the IT outsourcing risks effectively."

According to the PwC article on Service Provider Audits3, "Service provider audits are an essential tool for organizations to gain insight into their service providers' operations, controls, risks, and compliance status. Service provider audits can help organizations ensure that their service providers are meeting their expectations and obligations; identify any areas of improvement or concern; enhance their relationship and communication with their service providers; and optimize their IT outsourcing strategy."

Question: 506

Which of the following is the BEST approach to ensure global regulatory compliance when implementing a new business process?

A. Use a balanced scorecard to track the business process.
B. Ensure the appropriate involvement Of the legal department.
C. Review and revise the business architecture.
D. Seek approval from the change management board.

Answer: B

Explanation:

The best approach to ensure global regulatory compliance when implementing a new business process is to ensure the appropriate involvement of the legal department. The legal department is the function that provides legal advice and guidance to the organization on various matters, such as contracts, transactions, disputes, regulations, and compliance. By involving the legal department in the implementation of a new business process, the organization can ensure that the business process complies with the relevant laws, policies, and standards that apply in different countries and jurisdictions. The legal department can also help to identify and mitigate any legal risks or issues that may arise from the new business process, such as liability, litigation, or sanctions.

The other options are not as effective as ensuring the appropriate involvement of the legal department for ensuring global regulatory compliance when implementing a new business process. Using a balanced scorecard to track the business process is a good practice for measuring and evaluating the performance and value of the business process, but it does not guarantee compliance with global regulations. Reviewing and revising the business architecture is a necessary step for designing and aligning the business process with the business strategy and objectives, but it does not address the legal aspects of the business process. Seeking approval from the change management board is a relevant procedure for implementing a new business process, but it does not ensure that the change management board has the expertise or authority to assess and approve the global regulatory compliance of the business process.

Question: 507

A large enterprise is implementing an information security policy exception process. The BEST way to ensure that security risk is properly addressed is to:

confirm process owners' acceptance of residual risk.

perform an internal and external network penetration test.

obtain IT security approval on security policy exceptions.

A. benchmark policy against industry best practice.

Answer: A

Explanation:

The best way to ensure that security risk is properly addressed when implementing an information security policy exception process is to confirm process owners’ acceptance of residual risk. Residual risk is the risk that remains after applying controls or mitigating measures to reduce the original risk1. Process owners are the individuals or groups that are responsible for the design, execution, and performance of a business process2. By confirming process owners’ acceptance of residual risk, the enterprise can ensure that the security risk associated with the policy exception is understood, acknowledged, and agreed upon by the relevant stakeholders. This can also help to assign accountability and liability for the potential consequences of the policy exception, as well as to monitor and review the risk level and the effectiveness of the controls or mitigating measures. The other options are not as effective as confirming process owners’ acceptance of residual risk for ensuring that security risk is properly addressed when implementing an information security policy exception process. Performing an internal and external network penetration test is a useful technique for

identifying and exploiting vulnerabilities in the network infrastructure, but it does not address the specific security risk related to the policy exception. Obtaining IT security approval on security policy exceptions is a necessary step for validating and authorizing the policy exception, but it does not ensure that the process owners are aware of and accept the residual risk. Benchmarking policy against industry best practice is a good practice for comparing and improving the policy quality and performance, but it does not address the security risk associated with the policy exception.

Question: 508

A high-tech enterprise is concerned that leading competitors have been successfully recruiting top talent from the enterprise's research and development business unit.

What should the leadership team mandate FIRST?

A. A SWOT analysis
B. An incentive and retention program
C. A root cause analysis
D. An aggressive talent acquisition program

Answer: C

Explanation:

A root cause analysis is the first step to identify the factors that are causing the loss of top talent and to devise appropriate solutions. A SWOT analysis, an incentive and retention program, and an aggressive talent acquisition program are possible outcomes of a root cause analysis, but they are not the first action to take. Reference := CGEIT Review Manual, 7th Edition, page 103.

Question: 509

Which of the following metrics is MOST useful to ensure IT services meet business requirements?

A. Number of discontinued business transformation programs
B. Frequency Of IT services risk profile updates
C. Frequency Of IT policy updates
D. Number of business disruptions due to IT incidents

Answer: B

Explanation:

The frequency of IT services risk profile updates is a metric that measures how often the IT organization assesses and updates the risks associated with its services. This metric is useful to ensure that IT services meet business requirements, as it helps to identify and mitigate potential threats and vulnerabilities that could affect the availability, performance, reliability, and security of the services. A high frequency of IT services risk profile updates indicates that the IT organization is proactive and responsive to changing business needs and expectations. A low frequency of IT services risk profile updates suggests that the IT organization is reactive and complacent, and may not be aware of or prepared for emerging risks that could impact the business. Reference := Performance Measurement Metrics for IT Governance - ISACA, The 8 IT service management metrics that matter most

Question: 510

Which of the following is MOST important for a CIO to ensure before signing a contract for a new cloud-based customer relationship management (CRM) system?

The service provider has been audited for vulnerabilities and threats.

A. Risk management responsibilities are agreed upon and accepted.
B. The request for proposal (RFP) has been reviewed for completeness.
C. A full system functionality check has been completed.

Answer: B

Explanation:

Risk management is a crucial aspect of any cloud-based CRM system, as it involves identifying, assessing, and mitigating the potential risks that could affect the availability, performance, security, and compliance of the system. Before signing a contract for a new cloud-based CRM system, the CIO should ensure that the risk management responsibilities are clearly defined and allocated between the service provider and the customer, and that both parties accept and agree to them. This will help to avoid any confusion, conflict, or liability issues in case of any incidents or breaches that may occur in the future. Some of the risk management responsibilities that should be agreed upon and accepted are:

The scope and frequency of risk assessments and audits
The roles and responsibilities for risk monitoring and reporting
The escalation and resolution procedures for risk issues
The contingency and recovery plans for risk events
The security and privacy policies and standards for data protection
The service level agreements (SLAs) and key performance indicators (KPIs) for service quality and availability

Reference := Cloud-Based CRM: Best Practices for Implementation, The Best Contract Management Software, CRM Migration Best Practices: An Introductory Guide for HubSpot Agency Partners

Question: 511

Which of the following is the MOST efficient approach for using risk scenarios to evaluate a new business opportunity?

A. Related risks are consolidated into one scenario for analysis.
B. Risk events are identified bottom-up and top-down.
C. Risk identification leverages past audit and compliance reports.
D. Risk scenario narratives are summarized and limited in length.

Answer: B

Explanation:

The most efficient approach for using risk scenarios to evaluate a new business opportunity is to identify risk events from both bottom-up and top-down perspectives. This means that the risk identification process should consider both the specific details of the opportunity, such as the market, customer, product, service, technology, and resources involved, as well as the broader context of the opportunity, such as the strategic objectives, vision, mission, values, and culture of the organization. By using both bottom-up and top-down

approaches, the risk identification process can
capture a comprehensive and balanced view of the potential risks that could affect the success of the opportunity. This will help to create realistic and relevant risk scenarios that can be analyzed and evaluated for decision-making purposes. A bottom-up approach alone may miss some important risks that are related to the organization's strategy, governance, or environment, while a top-down approach alone may overlook some specific risks that are unique to the opportunity or its implementation. Therefore, a combination of both approaches is the most efficient way to use risk scenarios for evaluating a new business opportunity. Reference := What is business risk? | McKinsey, How to Write Strong Risk Scenarios and Statements - ISACA, Finding your blind spots: Recognising emerging risks and opportunities

Question: 512

Which of the following would BEST help to ensure the appropriate allocation of IT resources to support an enterprise's mission?

A. Develop a resource strategy as part of program management.
B. Prioritize program requirements based on existing resources.
C. Implement resource planning for each IT project.
D. Manage resources as part of the portfolio strategy.

Answer: D

Explanation:

Managing resources as part of the portfolio strategy would best help to ensure the appropriate allocation of IT resources to support an enterprise's mission. This is because the portfolio strategy aligns the IT investments with the business goals and priorities, and ensures that the IT resources are allocated to the most valuable and strategic initiatives. By managing resources at the portfolio level, the enterprise can optimize the use of its IT resources across multiple programs and projects, and avoid resource conflicts, shortages, or wastages. A resource strategy as part of program management, prioritizing program requirements based on existing resources,and resource planning for each IT project are all useful practices, but they are not sufficient to ensure the appropriate allocation of IT resources at the enterprise level. They may only focus on the resource needs and constraints of specific programs or projects, and may not consider the overall alignment and optimization of IT resources with the enterprise's mission. Reference := IT Portfolio Management: A Practitioner's Guide - ISACA, Resource Allocation Done Right: Best Practices for 2022 & Beyond, A Complete Guide to Resource Allocation in Projects - Float

Question: 513

A regulatory audit of an IT department has identified discrepancies between processes described in the procedures and what is actually done by system administrators.

The discrepancies were caused by recent IT application changes. Which of the following would be the BEST way to prevent the recurrence of similar findings in the future?

A. Assign the responsibility for periodic revisions and changes to process owners.
B. Require each IT employee to confirm compliance with IT procedures on an annual basis.
C. Include the update of documentation within the change management framework.

D. Establish high-level procedures to minimize process changes.

Answer: C

Explanation:

Including the update of documentation within the change management framework is the best way to prevent the recurrence of similar findings in the future. This is because the change management framework is a systematic and structured approach to managing changes in IT systems, applications, processes, and procedures. By incorporating the update of documentation as part of the change management process, the IT department can ensure that any changes are properly documented and communicated to the relevant stakeholders, and that the documentation is always aligned with the actual practices. This will help to avoid any discrepancies or inconsistencies between the procedures and what is actually done by system administrators, and thus reduce the risk of audit findings or noncompliance issues. Assigning the responsibility for periodic revisions and changes to process owners, requiring each IT employee to confirm compliance with IT procedures on an annual basis, and establishing high-level procedures to minimize process changes are all possible measures to improve the documentation quality, but they are not as effective or efficient as including the update of documentation within the changemanagement framework. They may not address the root cause of the problem, which is the lack of coordination and integration between the documentation and the change management activities. Reference := Change Management Best Practices for IT Teams - Smartsheet, IT Documentation: Purpose and Best Practices - Helpjuice, IT Documentation Best Practices | IT Glue

Question: 514

Which of the following has the GREATEST impact on the design of an IT governance framework?

A. IT performance metrics
B. Resource allocation
C. Business leadership
D. Business risk

Answer: D

Explanation:

Business risk has the greatest impact on the design of an IT governance framework, as it determines the level of control, oversight, and alignment that is required for the IT function to support the business objectives and mitigate the potential threats and vulnerabilities. Business risk is influenced by various factors, such as the industry, market, customer, competitor, regulatory, and environmental context of the enterprise. Therefore, the IT governance framework should be tailored to suit the specific risk profile and appetite of the enterprise, and to address the key risk areas and scenarios that could affect the business performance and value. According to COBIT 2019, one of the design factors that can influence the design of an enterprise's governance system is the risk profile1. This design factor reflects the degree of risk exposure and tolerance that the enterprise has in relation to its use of information and technology1. The risk profile can be assessed by considering various aspects, such as the likelihood and impact of risk events, the sources and types of risks, the risk

appetite and thresholds, the risk management capabilities and maturity, and the risk culture and awareness1. Based on the risk profile, the enterprise can decide on the appropriate governance objectives, components, enablers, practices, and activities that are needed to manage and mitigate the risks effectively1. The other options, IT performance metrics, resource allocation, and business leadership, are also important for the design

of an IT governance framework, but they are not as impactful as business risk. IT performance metrics are used to measure and monitor the effectiveness and efficiency of the IT function in delivering value to the business2. Resource allocation is a process that optimizes the use of IT resources across multiple programs and projects in alignment with the business goalsand priorities3. Business leadership is a role that provides strategic direction, guidance, and support for the IT function in achieving its objectives4. However, these factors are more related to the implementation and execution of the IT governance framework, rather than its design. They are also influenced by the business risk factor, as they depend on the level of risk exposure and tolerance that the enterprise has. Reference := IT Governance: Definitions, Frameworks and Planning - ProjectManager, Resource Allocation Done Right: Best Practices for 2022 & Beyond, The Role of Business Leadership in Effective IT Governance, COBIT Design Factors: A Dynamic Approach to Tailoring Governance in … - ISACA

Question: 515

An enterprise has made the strategic decision to begin a global expansion program which will require opening sales offices in countries across the world. Which of the following should be the FIRST consideration with regard to the IT service desk which will remain centralized?

The effect of regional differences On service delivery

Identification of IT service desk functions that can be outsourced

A. Enforcement Of a standardized policy across all regions
B. Availability of adequate resources to provide support for new users

Answer: A

Explanation:

The first consideration with regard to the IT service desk that will remain centralized is the effect of regional differences on service delivery. This is because regional differences can pose various challenges and opportunities for the IT service desk, such as:

Language and cultural barriers: The IT service desk staff should be able to communicate effectively and respectfully with customers from different countries and backgrounds, and understand their needs, preferences, and expectations. This may require hiring multilingual staff, providing language training, using translation tools, or outsourcing some services to local providers1.

Time zone differences: The IT service desk should be able to provide timely and consistent support to customers across different time zones, and avoid delays or disruptions in service delivery. This may require extending the service hours, implementing shift work, using automation tools, or outsourcing some services to local providers2.

Legal and regulatory differences: The IT service desk should be aware of and comply with the local laws and regulations that apply to the IT services they provide, such as data protection, privacy, security, taxation, and consumer rights. This may require conducting a risk assessment, obtaining legal advice, implementing policies and procedures, or outsourcing some services to local

providers3.

Technical and operational differences: The IT service desk should be able to adapt to the technical and operational requirements and challenges of the different regions they serve, such as network connectivity, bandwidth, infrastructure, devices, software, standards, and best practices. This may require conducting a feasibility study, investing in technology upgrades, implementing quality assurance measures, or

outsourcing some services to local providers4.

The other options, identification of IT service desk functions that can be outsourced, enforcement of a standardized policy across all regions, and availability of adequate resources to provide support for new users are also important considerations for the IT service desk that will remain centralized, but they are not the first one. They are more related to the implementation and execution of the IT service desk strategy, rather than its design. They are also influenced by the regional differences factor, as they depend on the level of variation and complexity that the IT service desk faces in different regions. Reference := Five Ways to Provide a World Class Service Desk Experience, How to Run an IT Service Desk in a Hybrid or Remote World - Gartner, Best Practices for Building a Service Desk | Atlassian, The Top 18 Help Desk Metrics and Best Practices - HubSpot Blog

Question: 516

In a large enterprise, which of the following is the BEST approach to enable effective communication to senior management regarding the project status for a strategic enterprise resource management system implementation?

A. Project management office with business and IT representatives
B. Weekly project reports reviewed by business and IT management
C. Project status updates on the intranet
D. A steering committee involving business and IT

Answer: D

Explanation:

A steering committee involving business and IT is the best approach to enable effective communication to senior management regarding the project status for a strategic enterpriseresource management system implementation. This is because a steering committee is a group of senior executives, stakeholders, and experts who provide strategic direction, guidance, and oversight for the project1. A steering committee can help to:

Communicate the project vision, goals, benefits, and risks to senior management and other stakeholders1
Monitor and review the project progress, performance, quality, and deliverables1
Resolve any issues, conflicts, or changes that may arise during the project1
Ensure the alignment of the project with the business strategy, objectives, and priorities1
Provide support, resources, and sponsorship for the project1

A steering committee involving business and IT can ensure that both the functional and technical aspects of the project are well represented and communicated to senior management. This can help to avoid any misunderstandings, gaps, or misalignments between the business and IT perspectives. A steering committee can also facilitate effective communication among senior management, project team, and other stakeholders, and foster a collaborative and supportive environment for the project success2.

The other options, project management office with business and IT representatives, weekly project reports reviewed by business and IT management, and project status updates on the intranet are not as effective as a steering committee for enabling communication to senior management regarding the project status. A project management office is a centralized unit that provides standards, methodologies, tools, and support for project management3. A project management office can help to improve the efficiency and consistency of project delivery, but it does not have the authority or responsibility to communicate directly with senior management or influence their decisions3. Weekly project reports are documents that summarize the progress, performance, issues, and risks

of a project in a given period4. Weekly project reports can help to keep senior management informed of the project status, but they may not be sufficient to address their concerns or expectations. Weekly project reports may also be too frequent or detailed for senior management who may prefer a higher-level or less frequent view of the project4. Project status updates on the intranet are web-based messages that provide information about the current state of a project5. Project status updates on the intranet can help to increase the visibility and transparency of the project status to senior management and other stakeholders, but they may not be effective in engaging them or soliciting their feedback. Project status updates on the intranet may also be overlooked or ignored by senior management who may have limited time or access to the intranet5. Reference := What is a Project Steering Committee? | Clarizen, How To Run An Effective Steering Committee Meeting - BrightWork, What Is a Project Management Office (PMO)? | Smartsheet, How To Write A Project Status Report: The Ultimate Guide, Project Status Update Email Sample : Templates and Examples

Question: 517

An internal audit of a large financial institution found that financial data is being managed in a way that will negatively impact the enterprise's ability to support regulatory reporting. Which of the following should be the FIRST strategic action in addressing this situation?

Establish a data governance framework.
Assign data responsibilities through a RACI chart.

Review key risk indicators (KRIS) related to data management.

A. Update data management policies.

Answer: A

Explanation:

Establishing a data governance framework is the first strategic action in addressing the situation where financial data is being managed in a way that will negatively impact the enterprise's ability to support regulatory reporting. This is because a data governance framework is a structured approach to managing and utilizing data in an organization. It includes policies, procedures, and standards that guide how data is collected, stored, managed, and used1. A data governance framework can help to: Improve data quality, accuracy, consistency, and completeness1
Ensure data privacy, security, and compliance with regulatory requirements1
Align data with business strategy, objectives, and priorities1
Enhance data integration, accessibility, and usability1
Define data roles and responsibilities and assign accountability1
By establishing a data governance framework, the enterprise can address the root cause of the

problem, which is the lack of control and oversight over the financial data. A data governance framework can help to ensure that the financial data is properly managed and utilized to support regulatory reporting and other business needs.
The other options, assigning data responsibilities through a RACI chart, reviewing key risk indicators (KRIs) related to data management, and updating data management policies are not as effective as establishing a data governance framework for addressing the situation. They are more related to the implementation and execution of the data governance framework, rather than its design. They are also dependent on the existence of a data governance framework, as they require a clear understanding of the data landscape, goals, and

standards of the organization.

Question: 518

IT governance within an enterprise is attempting to drive a cultural shift to enhance compliance with IT security policies. The BEST way to support this objective is to ensure that enterprise IT policies are:

A. communicated on a regular basis.
B. acknowledged and signed by each employee.
C. centrally posted and contain detailed instructions.
D. integrated into individual performance objectives.

Answer: D

Explanation:

Integrating IT security policies into individual performance objectives is the best way to support the objective of driving a cultural shift to enhance compliance with IT security policies. This is because performance objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what each employee is expected to accomplish and how they will be evaluated1. By integrating IT security policies into performance objectives, the enterprise can:

Communicate the importance and value of IT security policies to each employee2 Motivate and incentivize employees to comply with IT security policies2 Monitor and measure employees' compliance with IT security policies2

Provide feedback and recognition to employees who comply with IT security policies2

Identify and address any gaps or issues in employees' compliance with IT security policies2 Integrating IT security policies into performance objectives can help to create a culture of accountability, responsibility, and awareness for IT security within the enterprise. It can also help to align the individual goals of employees with the organizational goals of IT governance.

The other options, communicating IT security policies on a regular basis, acknowledging and signing IT security policies by each employee, and centrally posting IT security policies with detailed instructions are not as effective as integrating IT security policies into performance objectives for supporting the objective of driving a cultural shift to enhance compliance with IT security policies. They are more related to the dissemination and implementation of IT security policies, rather than their integration and evaluation. They may not have a significant impact on the behavior and attitude of employees towards IT security policies, as they may not provide sufficient motivation, feedback, or recognition for compliance. They may also be perceived as passive, formal, or coercive methods of enforcing IT security policies, rather than active, informal, or collaborative methods of engaging employees in IT security policies. Reference := Performance Objectives - SMART Goals - BusinessBalls, How toIntegrate Security Into Employee Performance Objectives, IT Security Policy: Key Components & Best Practices for Every Business …

Question: 519

An enterprise learns that some of its business divisions have been approaching technology vendors for cloud services, resulting in duplicate support contracts and underutilization of IT services. Which of the following should be done FIRST to address this issue?

A. Review the enterprise IT procurement policy.
B. Re-negotiate contracts with vendors to request discounts.
C. Require updates to the IT procurement process.

D. Conduct an audit to investigate utilization of cloud services.

Answer: A

Explanation:

The first thing that should be done to address the issue of duplicate support contracts and underutilization of IT services is to review the enterprise IT procurement policy. This is because the IT procurement policy is a document that defines the rules, guidelines, and procedures for acquiring and managing IT products and services in an organization1. A well-designed IT procurement policy can help to:

Align IT procurement with business strategy, objectives, and priorities1

Optimize IT spending and maximize IT value1

Ensure IT quality, security, and compliance1

Avoid IT duplication, waste, and inefficiency1

Define IT roles and responsibilities and assign accountability1

By reviewing the enterprise IT procurement policy, the organization can identify and address any gaps, issues, or inconsistencies that may have led to the problem of business divisions approaching technology vendors for cloud services without proper coordination or approval. The review can also help to update and improve the IT procurement policy to reflect the current and future needs and expectations of the organization and its stakeholders. Some of the best practices for developing an effective IT procurement policy are2:

Involve all relevant stakeholders in the policy development process Conduct a thorough analysis of the current and future IT requirements Establish clear criteria and standards for selecting and evaluating IT vendors and services Implement a robust approval and authorization system for IT purchases Incorporate risk management and contingency planning into the policy Communicate and educate the policy to all employees and stakeholders Monitor and measure the policy implementation and outcomes

The other options, re-negotiating contracts with vendors to request discounts, requiring updates to the IT procurement process, and conducting an audit to investigate utilization of cloud services are not as effective as reviewing the enterprise IT procurement policy for addressing the issue. They are more related to the implementation and execution of the IT procurement policy, rather than its design. They may also be reactive or corrective measures, rather than proactive or preventive ones. They may not address the root cause of the problem, which is the lack of a clear and comprehensive IT procurement policy that guides and governs the acquisition and management of IT products and services in the organization.

Question: 520

Which of the following is the BEST way for a CIO to provide progress updates on a newly implemented IT strategic plan to the board of directors?

Present an IT summary dashboard.

Present IT critical success factors (CSFs).

Report results Of key risk indicators (KRIs).

A. Report results of stage-gate reviews.

Answer: A

Explanation:

An IT summary dashboard is the best way for a CIO to provide progress updates on a newly implemented IT strategic plan to the board of directors, because it can help to communicate the key

performance indicators (KPIs), benefits, risks, and issues of the IT strategic plan in a concise, visual, and interactive way. An IT summary dashboard can also help to align the IT strategic plan with the business strategy, value creation, and stakeholder expectations, and demonstrate the value and contribution of IT to the enterprise. Presenting IT critical success factors (CSFs), reporting results of key risk indicators (KRIs), and reporting results of stage-gate reviews are not as effective as presenting an IT summary dashboard, because they are more focused on specific aspects of the IT strategic plan, rather than providing a holistic and comprehensive overview. Reference: IT Governance Dashboard, ISACA
What is an IT Dashboard?, Smartsheet
IT Strategy Dashboard, ClearPoint Strategy

Question: 521

After experiencing poor recovery times following a catastrophic event, an enterprise is seeking to improve its disaster recovery capabilities. Which of the following would BEST enable the enterprise to accomplish this objective?

A. Continuous testing of disaster recovery capabilities with implementation of lessons learned
B. Increased training and monitoring for disaster recovery personnel who perform below expectations
C. Annual review and updates to the disaster recovery plan (DRP)
D. Increased outsourcing of disaster recovery capabilities to ensure reliability

Answer: A

Explanation:

This is because continuous testing of disaster recovery capabilities can help to evaluate and validate the effectiveness and efficiency of the disaster recovery plan, identify and address any gaps or issues, and implement any improvements or adjustments based on the lessons learned1. Continuous testing can also help to ensure that the disaster recovery plan is aligned with the current and future business needs and expectations, and that the disaster recovery team and stakeholders are familiar and prepared with their roles and responsibilities1.

B . Increased training and monitoring for disaster recovery personnel who perform below expectations. This is not the best way to enable the enterprise to accomplish the objective of improving its disaster recovery capabilities, as it only focuses on one aspect of the disaster recovery plan, which is the human factor. While training and monitoring are important for enhancing the skills and performance of the disaster recovery personnel, they are not sufficient to address the other aspects of the disaster recovery plan, such as the technology, process, and communication factors2. Moreover, increased training and monitoring may not be effective if they are not based on a clear and comprehensive assessment of the disaster recovery capabilities and outcomes.

C . Annual review and updates to the disaster recovery plan (DRP). This is not the best way to enable the enterprise to accomplish the objective of improving its disaster recovery capabilities, as it may not be frequent or timely enough to capture and respond to the changing business environment and requirements. An annual review and update may also be insufficient to test and validate the disaster recovery plan, as it may not cover all possible scenarios or situations that could occur in a real disaster3. A more agile and adaptive approach to reviewing and updating the disaster recovery plan is recommended, such as using a continuous improvement cycle or a stage-gate process4.

D . Increased outsourcing of disaster recovery capabilities to ensure reliability. This is not the best way to enable the enterprise to accomplish the objective of improving its disaster recovery capabilities, as it may

introduce new risks and challenges for the enterprise, such as loss of control, dependency, compatibility, security, compliance, and cost issues5. Outsourcing some or all of the disaster recovery capabilities may also reduce the involvement and ownership of the enterprise's internal staff and stakeholders in the disaster recovery planning process, which could affect their commitment and readiness in case of a disaster5. Outsourcing should be carefully considered and evaluated based on the specific needs and circumstances of the enterprise, and should be complemented by a robust governance and management framework5.

Question: 522

Which of the following is the PRIMARY reason to monitor data classification efforts?

A. To identify and minimize data security breaches
B. To identify deviations in the data that are outside risk thresholds
C. TO ensure alignment with data protection regulations
D. To ensure assets are protected appropriately

Answer: B

Explanation:

The primary reason to monitor data classification efforts is to identify deviations in the data that are outside risk thresholds. This is because data classification is a process of organizing and labeling data according to its type, sensitivity, and value to the organization1. Data classification helps to ensure that data is protected and handled appropriately according to its risk level and compliance requirements1. By monitoring data classification efforts, the organization can:

Detect and prevent any unauthorized access, modification, or disclosure of sensitive or confidential data2
Identify and mitigate any potential threats or vulnerabilities that could affect the availability, integrity, or quality of data2
Evaluate and improve the effectiveness and efficiency of data classification policies, procedures, and tools2
Ensure alignment and consistency of data classification across different systems, applications, and processes2
Report and communicate the status and results of data classification to relevant stakeholders2 Monitoring data classification efforts can help the organization to manage and reduce the risks associated with data and to comply with relevant industry-specific regulatory mandates such as SOX, HIPAA, PCI DSS, and GDPR1.
Reference := Data Classification: Overview and Best Practices | Ground Labs, What Is Data Classification? The 5 Step Process & Best Practices for Classifying Data | Splunk

Question: 523

Which of the following is the MOST efficient way for an IT transformation project manager to communicate the project progress with stakeholders?

Establish governance forums within project management.

A. Include key performance indicators (KPIs) in a monthly newsletter.
B. Share the business case with stakeholders.
C. Post the project management report to the enterprise intranet site.

Answer: B

Explanation:

The most efficient way for an IT transformation project manager to communicate the project progress with stakeholders is to include key performance indicators (KPIs) in a monthly newsletter. This is because KPIs are measurable values that indicate how well the project is achieving its objectives and delivering value to the business1. By including KPIs in a monthly newsletter, the project manager can:

Provide a concise, clear, and consistent overview of the project status and results to the stakeholders2

Highlight the project achievements, challenges, and opportunities2

Demonstrate the alignment of the project with the business strategy, goals, and priorities2

Solicit feedback and suggestions from the stakeholders2

Foster a sense of engagement and collaboration among the stakeholders2

A monthly newsletter is an efficient communication channel, as it can reach a large and diverse audience of stakeholders, such as senior executives, business managers, IT staff, customers, and partners. It can also be easily distributed and accessed through email or intranet. A monthly frequency is appropriate for communicating the project progress, as it can provide timely and relevant information without overwhelming or distracting the stakeholders.

The other options, establishing governance forums within project management, sharing the business case with stakeholders, and posting the project management report to the enterprise intranet site are not as efficient as including KPIs in a monthly newsletter for communicating the project progress with stakeholders. They are more related to the planning and execution of the project, rather than its communication. They may also be too formal, detailed, or infrequent for some stakeholders who may prefer a more informal, concise, or frequent view of the project progress.

Question: 524

An enterprise's board of directors is developing a strategy change. Although the strategy is not finalized, the board recognizes the need for IT to be responsive. Which of the following is the FIRST step to prepare for this change?

A. Ensure IT has knowledgeable representation and is included in the strategic planning process.

B. Increase the IT budget and approve an IT staff level increase to ensure resource availability for the strategy change.

C. Initiate an IT service awareness campaign to business system owners and implement service level agreements (SLAs).

D. Outsource both IT operations and IT development and implement controls based on a standardized framework.

Answer: A

Explanation:

This is because IT is a key enabler and driver of business strategy, and it needs to understand and align with the strategic vision, goals, and priorities of the enterprise1. By ensuring IT has knowledgeable representation and is included in the strategic planning process, the enterprise can: Leverage IT's expertise and insights to identify and evaluate the opportunities and challenges of the strategy change1

Ensure IT's readiness and capability to support and execute the strategy change1

Avoid any gaps or misalignments between IT and business expectations and requirements1 Foster a collaborative and supportive relationship between IT and business stakeholders1 B . Increase the IT budget and approve an IT staff level increase to ensure resource availability for the strategy change. This is not the first

step to prepare for the change in the enterprise's board of directors' strategy, as it may be premature or unnecessary to do so without a clear understanding and agreement of the scope, impact, and implications of the strategy change. Increasing the IT budget and staff level may also create inefficiencies or wastages if they are not aligned with the actual needs and priorities of the strategy change2.

C . Initiate an IT service awareness campaign to business system owners and implement service level agreements (SLAs). This is not the first step to prepare for the change in the enterprise's board of directors' strategy, as it may not be relevant or effective to do so without a clear definition and communication of the strategy change. Initiating an IT service awareness campaign and implementing SLAs are more related to the delivery and management of IT services, rather than the planning and alignment of IT strategy3.

D . Outsource both IT operations and IT development and implement controls based on a standardized framework. This is not the first step to prepare for the change in the enterprise's board of directors' strategy, as it may introduce new risks and challenges for IT governance, such as loss of control, dependency, compatibility, security, compliance, and cost issues4. Outsourcing both IT operations and development may also reduce the involvement and ownership of IT in the strategic planning process, which could affect its alignment and responsiveness to the strategy change4. Outsourcing should be carefully considered and evaluated based on the specific needs and circumstances of the enterprise, and should be complemented by a robust governance and management framework4.

Question: 525

Which of the following is the PRIMARY consideration for an enterprise when deciding whether to adopt a qualitative risk assessment method?

The method identifies areas to immediately address vulnerabilities.

The method provides specific objective measurements of exposure.

The method enables an analysis Of recommended controls.

A. The method provides a platform for all departments to contribute to the risk assessment.

Answer: A

Explanation:

The primary consideration for an enterprise when deciding whether to adopt a qualitative risk assessment method is:

The level of detail and accuracy required for the risk assessment. Qualitative risk assessment is a method that uses scenarios, subjectivity, and knowledge to evaluate risks. It does not provide specific objective measurements of exposure, but rather a relative ranking or rating of risks based on their likelihood and impact1. Qualitative risk assessment is suitable for situations where the data is scarce, uncertain, or incomplete, or where the risk assessment needs to be done quickly and easily1. However, qualitative risk assessment may also be biased, inconsistent, or inaccurate, as it depends on the judgment and experience of the risk assessors1. Therefore, an enterprise should consider the level of detail and accuracy required for the risk assessment before choosing a qualitative method. If the enterprise needs more precise and reliable estimates of risk exposure, it may opt for a quantitative method instead1.

The other options are not the primary consideration for an enterprise when deciding whether to adopt a qualitative risk assessment method. The method identifies areas to immediately address vulnerabilities, enables an analysis of recommended controls, and provides a platform for all departments to contribute to the risk assessment are all possible benefits or outcomes of using a qualitative risk assessment method, but they

are not the main factor that influences the decision to use it. They may also apply to other methods of risk assessment, such as quantitative or hybrid methods2.

Question: 526

Which of the following is the BEST way for a CIO to ensure that IT-related training is taken seriously by the IT management team and direct employees?

A. Develop training programs based on results of an IT staff survey of preferences.
B. Embed training metrics into the annual performance appraisal process.
C. Promote IT-specific training awareness program.
D. Research and identify training needs based on industry trends.

Answer: B

Explanation:

This is because training metrics are measurable values that indicate the effectiveness and impact of the training programs on the IT staff's knowledge, skills, and performance1. By embedding training metrics into the annual performance appraisal process, the CIO can: Communicate the importance and value of IT-related training to the IT management team and direct employees2
Motivate and incentivize the IT management team and direct employees to participate in and complete the IT-related training2
Monitor and evaluate the IT management team and direct employees' progress, achievement, and improvement in the IT-related training2
Provide feedback and recognition to the IT management team and direct employees who excel in the IT-related training2
Identify and address any gaps or issues in the IT-related training or its outcomes2
Embedding training metrics into the annual performance appraisal process can help to create a culture of learning, development, and accountability for IT-related training within the organization. It can also help to align the individual goals of the IT management team and direct employees with the organizational goals of IT governance.
The other options, developing training programs based on results of an IT staff survey of preferences, promoting IT-specific training awareness program, and researching and identifying training needs based on industry trends are not as effective as embedding training metrics into the annual performance appraisal process for ensuring that IT-related training is taken seriously by the IT management team and direct employees. They are more related to the design and delivery of the IT- related training, rather than its integration and evaluation. They may also not have a significant impact on the behavior and attitude of the IT management team and direct employees towards IT- related training, as they may not provide sufficient motivation, feedback, or recognition for participation or completion.

Question: 527

An enterprise is implementing its first mobile sales channel. Final approval for accepting the associated IT risk should be obtained from which of the following?

Risk manager

Business sponsor

A. Chief information officer (CIO)
B. IT steering committee

Answer: B

Explanation:

Final approval for accepting the associated IT risk should be obtained from the business sponsor. This is because the business sponsor is the person or group who initiates, funds, and owns the business case for the mobile sales channel project1. The business sponsor is responsible for defining the business objectives, benefits, and requirements of the project, and for ensuring its alignment with the enterprise strategy1. The business sponsor is also accountable for the outcomes and value of the project, and for managing the risks and issues that may affect its success1. Therefore, the business

sponsor should have the authority and responsibility to approve the IT risk associated with the mobile sales channel project, as it may impact the business performance and value.

The other options, risk manager, chief information officer (CIO), and IT steering committee are not the best choices for obtaining final approval for accepting the associated IT risk. They are more involved in the identification, assessment, mitigation, and monitoring of IT risks, rather than their acceptance2. They may also have different perspectives and interests than the business sponsor regarding the IT risk associated with the mobile sales channel project. For example, the risk manager may focus on minimizing or avoiding IT risks, while the CIO may focus on maximizing or exploiting IT opportunities. The IT steering committee may have a broader view of IT risks across multiple projects and programs, rather than a specific one. Therefore, they may not have the final say or decision on accepting the IT risk associated with the mobile sales channel project.

Question: 528

Which of the following roles is directly responsible for information quality?

A. Information custodian
B. Information steward
C. Information analyst
D. Information owner

Answer: B

Explanation:

This is because an information steward is a person or group who is accountable for the quality, integrity, and usability of the information assets within a specific domain or function1. The responsibilities of an information steward include the following1:

Defining and enforcing data quality standards, policies, and procedures Monitoring and measuring data quality performance and outcomes Identifying and resolving data quality issues and errors
Collaborating with data owners, custodians, analysts, and users to ensure data quality alignment and improvement
Educating and training data stakeholders on data quality best practices and tools
An information steward plays a key role in ensuring that the information assets are accurate, complete, consistent, reliable, and fit for purpose1.

The other options, information custodian, information analyst, and information owner are not directly responsible for information quality. They are more involved in the creation, storage, access, and use of information assets, rather than their quality2. They may also have different perspectives and interests than the information steward regarding the information quality. For example, the information custodian may focus on the security and availability of information assets, while the information analyst may focus on the analysis and interpretation of information assets. The information owner may focus on the value and benefits of information assets. Therefore, they may not have the same authority or responsibility as the information steward for ensuring information quality. Reference := What Is an Information Steward? | Informatica, Data Roles: Data Owner vs Data Steward vs Data Custodian

Question: 529

Which of the following would BEST help assess the effectiveness of a newly established IT governance framework?

A. Develop a business case for the program portfolio.
B. Evaluate key performance indicator (KPI) results.
C. Benchmark the IT governance framework to industry best practice.
D. Review results of IT audit reports.

Answer: B

Explanation:

This is because KPIs are measurable values that indicate how well the IT governance framework is achieving its objectives and delivering value to the business1. By evaluating KPI results, the organization can: Monitor and review the IT governance framework's progress, performance, quality, and outcomes Highlight the IT governance framework's achievements, challenges, and opportunities
Demonstrate the alignment of the IT governance framework with the business strategy, goals, and priorities Provide recommendations and feedback for the IT governance framework's improvement and adjustment Evaluating KPI results can provide a comprehensive and objective overview of the IT governance framework's effectiveness and impact.
The other options, developing a business case for the program portfolio, benchmarking the IT governance framework to industry best practice, and reviewing results of IT audit reports are not as effective as evaluating KPI results for assessing the effectiveness of a newly established IT governance framework. They are more related to the design and implementation of the IT governance framework, rather than its evaluation. They may also be too narrow or subjective for assessing the IT governance framework's effectiveness, as they may not cover all aspects or perspectives of the IT governance framework. They may also depend on external factors or standards that may not be relevant or applicable to the organization's specific context and needs.

Question: 530

An organization requires updates to their IT infrastructure to meet business needs. Which of the following will provide the MOST useful information when planning for the necessary IT investments?

A. Enterprise architecture (EA)
B. Risk assessment report
C. Business user satisfaction metrics
D. Audit findings

Answer: A

Explanation:

This is because enterprise architecture (EA) is a practice that helps organizations align their IT systems and processes with their business objectives. EA provides a holistic and integrated viewof the current and future state of the organization's IT infrastructure, as well as the gaps, issues, and opportunities for improvement1. By using EA, the organization can:

Identify and prioritize the IT investments that support the business strategy, goals, and needs1 Optimize the IT spending and maximize the IT value1

Ensure the IT quality, security, and compliance1

Avoid IT duplication, waste, and inefficiency1

Define IT roles and responsibilities and assign accountability1

EA can help the organization plan for the necessary IT investments in a systematic and structured way, and ensure that they are aligned with the business vision and value.

The other options, risk assessment report, business user satisfaction metrics, and audit findings are not as useful as enterprise architecture (EA) for planning for the necessary IT investments. They are more related to the evaluation and monitoring of the IT performance, rather than the planning and alignment of the IT strategy. They may also provide limited or partial information about the IT infrastructure, rather than a comprehensive and integrated view. They may also depend on external factors or standards that may not be relevant or applicable to the organization's specific context and needs.

Question: 531

Which of the following is the BEST indication that an implementation plan for a new governance initiative will be successful?

A. Staff have been trained on the new initiative.
B. External consultants created the plan.
C. The plan assigns responsibility for completing milestones.
D. The plan is designed to engage employees across the enterprise.

Answer: D

Explanation:

This is because employee engagement is a key factor for the success of any change initiative, especially one that involves governance. Employee engagement refers to the degree of commitment, involvement, and ownership that employees have toward the organization and its goals1. By designing the implementation plan to engage employees across the enterprise, the organization can:

Communicate the vision, purpose, and benefits of the new governance initiative to employees2 Solicit feedback and suggestions from employees on how to implement the new governance initiative effectively2

Address any concerns or resistance that employees may have toward the new governance initiative2 Empower and motivate employees to participate in and support the new governance initiative2 Foster a culture of collaboration, learning, and innovation among employees2

Designing the implementation plan to engage employees across the enterprise can help to ensure that the new governance initiative is understood, accepted, and adopted by all stakeholders, and that it delivers the desired outcomes and value.

The other options, staff have been trained on the new initiative, external consultants created the plan, and the plan assigns responsibility for completing milestones are not as indicative as the plan is designed to engage

Watermark Sample

employees across the enterprise for the success of the implementation plan for a new governance initiative. They are more related to the execution and management of the implementation plan, rather than its design and alignment. They may also not be sufficient or effective for ensuring the success of the implementation plan, as they may not address the human and behavioral aspects of change, such as awareness, understanding, involvement, commitment, and ownership3. Reference := Employee Engagement: What Is It? | SHRM, How To Engage Employees In Organizational Change | Forbes, Change Management Best Practices: A Comprehensive Guide | Smartsheet

Question: 532

Which strategic planning approach would be MOST appropriate for a large enterprise to follow when revamping its IT services?

A. Addressing gaps within the management of IT-related risk
B. Focusing on business innovation through knowledge, expertise, and initiatives
C. Calibrating and scaling delivery Of IT services in line with business requirements
D. Adhering to on-time and on-budget IT service delivery

Answer: C

Explanation:

This is because calibrating and scaling delivery of IT services means adjusting and optimizing the IT service portfolio, processes, and resources to meet the changing and diverse needs and expectations of the business1. By following this approach, the large enterprise can: Align IT services with business strategy, objectives, and priorities1 Enhance IT service quality, efficiency, and effectiveness1 Improve IT service agility, flexibility, and responsiveness1 Reduce IT service costs, risks, and waste1 Increase IT service value, satisfaction, and innovation1

Calibrating and scaling delivery of IT services can help the large enterprise revamp its IT services in a way that supports and enables the business success.

The other options, addressing gaps within the management of IT-related risk, focusing on business innovation through knowledge, expertise, and initiatives, and adhering to on-time and on-budget IT service delivery are not as appropriate as calibrating and scaling delivery of IT services for a large enterprise to follow when revamping its IT services. They are more related to specific aspects or outcomes of IT service management, rather than a holistic and strategic approach. They may also be too narrow or rigid for a large enterprise that needs to adapt and evolve its IT services to the dynamic and complex business environment. They may not address the full scope or potential of IT service improvement and transformation.

Question: 533

From an IT governance perspective, which of the following would be the MOST significant impact of moving all IT applications to an external Software as a Service (SaaS) cloud provider?

A. The integration of the IT department with business lines
B. The shift from service delivery to service management
C. The improvement Of IT service alignment with business

D. The necessity to update key risk indicators (KRIs)

Answer: B

Explanation:

This is because moving all IT applications to an external SaaS cloud provider means that the organization is outsourcing the development, deployment, maintenance, and operation of its IT applications to a third-party vendor. This implies that the organization is relinquishing some control and ownership over its IT applications, and relying on the vendor to provide the required functionality, performance, quality, and security1. Therefore, the organization needs to shift its focus from delivering IT services internally to managing IT services externally. This involves the following activities2:

Establishing and maintaining a clear and comprehensive contract or service level agreement (SLA) with the SaaS vendor that defines the roles, responsibilities, expectations, and outcomes of both parties2

Monitoring and measuring the SaaS vendor's compliance with the contract or SLA, and ensuring that the vendor meets the agreed service levels, standards, and metrics2

Communicating and collaborating with the SaaS vendor regularly, and resolving any issues, conflicts, or changes that may arise during the service delivery2

Evaluating and improving the effectiveness and efficiency of the SaaS vendor's service delivery, and identifying and implementing any opportunities for innovation or optimization2

Managing the risks and challenges associated with outsourcing IT services to a SaaS vendor, such as data privacy, security, availability, compatibility, integration, dependency, cost, and performance issues2

The shift from service delivery to service management can have a significant impact on the IT governance framework, processes, policies, and practices of the organization. It can also affect the IT skills, roles, and responsibilities of the IT staff and stakeholders. Therefore, the organization needs to adapt and adjust its IT governance approach accordingly to ensure that it can effectively oversee and optimize its IT services in a SaaS environment3.

The other options, the integration of the IT department with business lines, the improvement of IT service alignment with business, and the necessity to update key risk indicators (KRIs) are not as significant as the shift from service delivery to service management for moving all IT applications to an external SaaS cloud provider from an IT governance perspective. They are more related to the outcomes or consequences of moving to a SaaS environment, rather than the impact or change itself. They may also not be unique or specific to a SaaS environment, as they may apply to other types or models of IT service delivery as well.

Question: 534

The GREATEST benefit associated with a decision to implement performance metrics for key IT assets is the ability to:

A. establish the span of control during the life cycle of IT assets.
B. determine the average cost of controls for protection of IT assets.
C. compare the performance Of IT assets against industry best practices.
D. determine the contribution of IT assets in achievement of IT goals.

Answer: D

Explanation:

This is because performance metrics are measurable values that indicate how well the IT assets are performing in terms of functionality, quality, efficiency, and effectiveness1. By implementing performance metrics for

key IT assets, the organization can:

Monitor and review the IT assets' progress, performance, quality, and outcomes Highlight the IT assets' achievements, challenges, and opportunities

Demonstrate the alignment of the IT assets with the IT strategy, goals, and priorities Provide recommendations and feedback for the IT assets' improvement and adjustment Implementing performance metrics for key IT assets can help the organization determine the contribution of IT assets in achievement of IT goals, and ensure that they deliver value to the business.

The other options, establishing the span of control during the life cycle of IT assets, determining the average cost of controls for protection of IT assets, and comparing the performance of IT assets against industry best practices are not as beneficial as determining the contribution of IT assets in achievement of IT goals for implementing performance metrics for key IT assets. They are more related to specific aspects or outcomes of IT asset management, rather than a holistic and strategic benefit. They may also not be relevant or applicable to all types or categories of IT assets. They may not address the full scope or potential of IT asset improvement and optimization. Reference := What Is an IT Asset Management KPI? | Filewave, Performance Measurement Metrics for IT Governance - ISACA

Question: 535

A small enterprise has just hired its first CIO, who has been tasked with making the IT department more efficient. What should be the CIO's NEXT step after identifying several new improvement initiatives?

A. Mandate IT staff training.
B. Request an IT balanced scorecard.
C. Require a cost-benefit analysis.
D. Allocate funding for the initiatives.

Answer: C

Explanation:

A cost-benefit analysis (CBA) is a process that's used to estimate the costs and benefits of projects or investments to determine their profitability for an organization. A CBA is a versatile method that's often used for business administration, project management and public policy decisions1. A CBA can help the CIO prioritize the improvement initiatives based on theirexpected value and feasibility, and justify the allocation of resources and funding for them. A CBA can also align the IT goals with the enterprise objectives and demonstrate the IT value delivery to the stakeholders2. Reference :=

2: CGEIT Exam Content Outline | ISACA

1: Cost-Benefit Analysis: A Quick Guide with Examples and Templates

Question: 536

Which of the following BEST enables an enterprise to determine whether a current program for IT infrastructure migration to the cloud is continuing to provide benefits?

A. Key performance indicators (KPIs)
B. Total cost of ownership (TCO)
C. Key risk indicators (KRIS)
D. Net present value (NPV)

Answer: A

Explanation:

Key performance indicators (KPIs) are metrics that measure the performance of a project, program, or investment against a set of targets, objectives, or benchmarks. KPIs can help an enterprise to determine whether a current program for IT infrastructure migration to the cloud is continuing to provide benefits by tracking the progress, efficiency, quality, and outcomes of the program. KPIs can also help to identify any gaps, issues, or risks that may affect the program's success and enable timely corrective actions12.

Total cost of ownership (TCO) is the purchase price of an asset plus the costs of operation over its life span. TCO can help an enterprise to compare the costs and benefits of different IT infrastructure options, such as cloud versus on-premise, but it does not measure the ongoing performance or benefits of a chosen option3.

Key risk indicators (KRIs) are metrics that monitor and predict potential risks that may negatively impact an enterprise's objectives or operations. KRIs can help an enterprise to identify and mitigate any risks associated with IT infrastructure migration to the cloud, such as security breaches, data loss, or service disruptions, but they do not measure the benefits or value of the program45.

Net present value (NPV) is the difference between the present value of cash inflows and the present value of cash outflows over a period of time. NPV is used to evaluate the profitability or return on investment of a project or investment by discounting the future cash flows to their present value. NPV can help an enterprise to decide whether to undertake an IT infrastructuremigration to the cloud based on its expected net value, but it does not measure the actual performance or benefits of the program16. Reference :=

3: Total Cost of Ownership: How It's Calculated With Example - Investopedia

4: Key Risk Indicators (KRIs) - National Treasury

2: How to Develop Key Risk Indicators (KRIs) to Fortify Your Business | AuditBoard

5: How to Develop Effective Key Risk Indicators - Secureframe

1: Net Present Value (NPV) - Definition, Examples, How to Do NPV Analysis

6: NPV Formula - Learn How Net Present Value Really Works, Examples

Question: 537

An enterprise is concerned that ongoing maintenance costs are not being considered when prioritizing IT-enabled business investments. Which of the following should be the enterprise's FIRST course of action?

A. Implement a balanced scorecard for the IT project portfolio.
B. Establish a portfolio manager role to monitor and control the IT projects.
C. Require business cases to have product life cycle information.
D. Mandate an enterprise architecture (EA) review with business stakeholders.

Answer: C

Explanation:

A product life cycle is the length of time from a product first being introduced to consumers until it is removed from the market. It consists of four or five stages, depending on the source: introduction, growth, maturity, decline, and sometimes development1. A product life cycle information can help the enterprise to estimate the ongoing maintenance costs of IT-enabled business investments, as well as their expected benefits, risks, and returns. By requiring business cases to have product life cycle information, the enterprise can prioritize IT-enabled business investments based on their longterm value and alignment with the enterprise's objectives2.

A balanced scorecard is a management system that clarifies the strategy and vision of an organization,

translating them into action that can be tracked. It uses four perspectives: financial, customer, internal business process, and knowledge, education, and growth3. A balanced scorecard for the IT project portfolio can help the enterprise to measure the performance and value of IT projects, but it does not necessarily consider the ongoing maintenance costs of IT-enabled business investments.

A portfolio manager is a specialized project manager who focuses on IT projects. They are responsible for keeping projects within budget, optimizing time management for IT teams, and allocating resources appropriately4. Establishing a portfolio manager role to monitor and control the IT projects can help the enterprise to manage its IT project portfolio more effectively, but it does not address the issue of prioritizing IT-enabled business investments based on their ongoing maintenance costs.

An enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. It describes the current and future state of the organization in terms of its strategy, processes, information systems, and technology infrastructure5. Mandating an EA review with business stakeholders can help the enterprise to align its IT-enabled business investments with its strategic goals and ensure compliance with defined security rules, but it does not solve the problem of considering the ongoing maintenance costs of IT-enabled business investments.

Question: 538

Which of the following would BEST help to prevent an IT system from becoming obsolete before its planned return on investment (ROI)?

A. Obtaining independent assurance that the IT system conforms to business requirements
B. Defining IT and business goals to ensure value delivery as required
C. Managing the benefit realization through the entire life cycle
D. Ordering an external audit for the IT system early in the roll out

Answer: C

Explanation:

To prevent an IT system from becoming obsolete before achieving its planned return on investment (ROI), it is crucial to manage the benefit realization throughout the entire lifecycle of the system. This approach involves continuously monitoring and adjusting the system to ensure it delivers the expected value and benefits from inception through decommissioning. This proactive management

helps in adapting to changes in technology and business environments, thus extending the relevance and utility of the IT system. Obtaining independent assurance,defining IT and business goals, and ordering an external audit are important practices but do not directly address the ongoing management of the system's value delivery and adaptability over time.

Question: 539

Despite an adequate training budget. IT staff are not keeping skills current with emerging technologies critical to the business. Which of the following is the BEST way for the enterprise to address this situation?

A. Provide incentives for IT staff to attend outside conferences and training
B. Create a standard-setting center of excellence for IT.
C. Require human resources (HR) to recruit new talent using an established IT skills matrix.
D. Establish an agreed-upon skills development plan with each employee

Answer: D

Explanation:

The best way to address the issue of IT staff not keeping their skills current, despite an adequate training budget, is to establish an agreed-upon skills development plan with each employee. This personalized approach ensures that training and development activities are directly aligned with both the organization's needs and the individual's career goals, thereby increasing the likelihood of participation and the application of new skills. While providing incentives and creating centers of excellence can be supportive, a tailored development plan directly engages each staff member in their growth, ensuring relevance and commitment.

Question: 540

Which of the following BEST facilitates the adoption of an IT governance program in an enterprise?

A. Defining clear roles and responsibilities for the participants
B. Using a comprehensive business case for the initiative
C. Communicating the planned IT strategy to stakeholders
D. Addressing the behavioral and cultural aspects of change

Answer: D

Explanation:

Facilitating the adoption of an IT governance program in an enterprise requires addressing the behavioral and cultural aspects of change. This approach recognizes that the success of such a program depends not only on the structural and strategic elements but also on how well the people within the organization accept and adapt to the changes. Addressing cultural aspects involves engaging stakeholders, fostering a governance mindset, and overcoming resistance to change, thereby ensuring a smoother and more effective implementation. While defining roles, building business cases, and communicating strategies are critical, they must be complemented by efforts to manage the human side of change.

Question: 541

When conducting a risk assessment in support of a new regulatory requirement, the IT risk committee should FIRST consider the: A. cost burden to achieve compliance.

B. readiness of IT systems to address the risk.
C. risk profile of the enterprise.
D. disruption to normal business operations.

Answer: C

Explanation:

When conducting a risk assessment in support of a new regulatory requirement, the IT risk committee should first consider the risk profile of the enterprise. Understanding the overall risk landscape, including existing vulnerabilities, threats, and the impact of potential risks, provides a foundation for evaluating how new regulatory requirements will affect the organization. This initial step ensures that subsequent risk management efforts, including compliance activities, are aligned with the enterprise's risk appetite and strategic objectives. While cost, system readiness, and operational disruption are important considerations, they should be evaluated in the context of the enterprise's risk profile.

Question: 542

An IT steering committee is concerned about staff saving data files containing sensitive corporate information on publicly available cloud file storage applications. Which of the following should be done FIRST to address this concern?

A. Create a secure corporate cloud file storage and sharing solution.
B. Block corporate access to cloud file storage applications.
C. Require staff training on data classification policies.
D. Revise the data management policy to prohibit this practice.

Answer: C

Explanation:

To address concerns about staff saving sensitive corporate information on publicly available cloud file storage applications, the first step should be to require staff training on data classification policies. Educating employees about the types of data classified as sensitive and the associated handling requirements helps to raise awareness and change behavior. Training should emphasize the importance of protecting sensitive information and the proper use of approved storage solutions. While creating secure storage solutions, blocking access to certain applications, and revising policies are important measures, education and awareness are fundamental first steps to ensure compliance and mitigate risks.

Question: 543

ACIO determines IT investment management processes are not fully realizing the benefits identified in business cases. Which of the following would be the BEST way to prevent this issue?

A. Establish a requirement for CIO review and approval of each business case.
B. Evaluate the delegation of investment approval authorities.
C. Perform stage-gate reviews throughout the life cycle of each project.
D. Document lessons learned throughout the investment life cycle.

Answer: C

Explanation:

Performing stage-gate reviews throughout the life cycle of each project is the best way to ensure IT investment management processes are fully realizing the benefits identified in business cases. Stagegate reviews provide structured checkpoints at critical phases of a project, allowing for the evaluation of progress, performance against objectives, and the continued viability and alignment with business goals. This approach enables timely adjustments to be made, ensuring that projects stay on track to deliver the expected benefits. While CIO review and approval, evaluating delegation of authority, and documenting lessons learned are valuable, they do not offer the continuous oversight and opportunity for course correction that stage-gate reviews do.

Question: 544

An enterprise's IT department has been operating independently without regard to business concerns, leading to misalignment between business and IT. The BEST way to establish alignment would be to require:

A. business to help define IT goals.
B. business to fund IT services.

C. IT to define business objectives.
D. IT and business to define risks.

Answer: A

Explanation:

Requiring the business to help define IT goals is the best way to establish alignment between business and IT when the IT department has been operating independently of business concerns. This collaborative approach ensures that IT initiatives are directly linked to business objectives, facilitating strategic alignment and ensuring that IT supports and enhances business operations. While IT defining business objectives, business funding IT services, and both defining risks are important, the foundational step for alignment is integrating business perspectives into the definition of IT goals.

Question: 545

Which of the following is the BEST way for a CIO to assess the consistency of IT processes against industry benchmarks to determine where to focus improvement initiatives?

A. Utilizing a capability maturity model
B. Evaluating the current balanced scorecard
C. Reviewing key performance measures
D. Reviewing IT process audit results

Answer: A

Explanation:

Utilizing a capability maturity model is the best way for a CIO to assess the consistency of IT processes against industry benchmarks and determine where to focus improvement initiatives. Capability maturity models provide a structured framework for evaluating the maturity of an organization's processes in comparison to industry best practices. This approach helps identify areas of strength and opportunities for improvement, guiding strategic decisions on where to allocate resources for process enhancements. While balanced scorecards, key performance measures, and IT process audit results are useful, a capability maturity model offers a comprehensive assessment specifically designed for process improvement.

Question: 546

Which of the following is the BEST indication of an effective information governance model?

A. Senior management ensures quality goals are defined for information.
B. The CIO defines information accountability, quality criteria, and criticality.
C. Enterprise architects define information protection attributes.
D. Process owners determine which information assets will be managed.

Answer: A

Explanation:

An effective information governance model is best indicated when senior management ensures that quality goals are defined for information. This top-down approach demonstrates a commitment to managing information as a strategic asset, with clear quality objectives that align with business goals. It ensures accountability and sets the tone for information governance practices across the organization. While the roles of the CIO, enterprise architects, and process owners are important, the involvement of senior management in defining quality goals is a key indicator of an effective governance model.

Question: 547

Which of the following BEST helps to ensure that IT policies are aligned with organizational strategies?

A. The policies are approved by the board of directors.
B. The policies are developed using a top-down approach.
C. The policies are updated annually.
D. The policies are periodically audited.

Answer: B

Explanation:

Ensuring that IT policies are aligned with organizational strategies is best achieved when the policies are developed using a top-down approach. This approach starts with strategic objectives and cascades down to operational policies, ensuring coherence and alignment with the overall direction and goals of the organization. While board approval, annual updates, and periodic audits are important for policy governance, the top-down development approach ensures that policies are inherently designed to support organizational strategies from the outset.

Question: 548

Within a governance structure for risk management, which of the following activities should be performed by the second line of defense?

A. Conducting internal and external audits
B. Implementing controls to manage risk
C. Monitoring risk and controls
D. Identifying and assessing risk

Answer: C

Explanation:

Within a governance structure for risk management, the second line of defense is primarily responsible for monitoring risk and controls. This function involves overseeing the effectiveness of the first line of defense (operational management and control implementation) and ensuring that risk management practices are properly integrated into business processes. It serves as a check on the adequacy and effectiveness of risk management across the organization. While conducting audits is a function of the third line of defense (internal audit), and identifying and assessing risk is often a shared responsibility, the distinct role of the second line is to provide ongoing monitoring and oversight of risk management and control processes.

Question: 549

Which of the following is the PRIMARY role of the CEO in IT governance?

A. Establishing enterprise strategic goals
B. Managing the risk governance process
C. Evaluating return on investment (ROI)
D. Nominating IT steering committee membership

Answer: A

Explanation:

The primary role of the CEO in IT governance is establishing enterprise strategic goals. The CEO is responsible for setting the vision and strategic direction of the organization, which includes ensuring that IT governance aligns with and supports these broader objectives. While managing the risk governance process, evaluating ROI, and nominating IT steering committee membership are important, these are typically shared responsibilities or delegated to other roleswithin the organization. The CEO's leadership in defining the strategic goals is fundamental to guiding all aspects of IT governance and ensuring alignment with the business strategy.

Question: 550

An IT governance committee realizes there are antiquated technologies in use throughout the enterprise. Which of the following is the BEST group to evaluate the recommendations to address these shortcomings?

A. Enterprise architecture (EA) review board
B. Business process improvement workgroup
C. Audit committee
D. Risk management committee

Answer: A

Explanation:

The best group to evaluate recommendations to address the use of antiquated technologies throughout the enterprise is the Enterprise Architecture (EA) review board. This group is responsible for overseeing the architectural framework and ensuring that IT systems and technologies align with the enterprise's strategic objectives. The EA review board has the expertise to assess the impact of current technologies on the business and recommend modernization strategies that align with the enterprise architecture. While business process improvement workgroups, audit committees, and risk management committees play important roles, the EA review board is specifically equipped to address technological shortcomings and alignment with business goals.

Question: 551

Which of the following would be an IT steering committee's BEST course of action upon learning business units have been independently procuring cloud services?

A. Require cancellation of cloud-based application services not vetted by IT leadership.
B. Include business unit leadership in the enterprise architecture (EA) review board.
C. Limit cloud-based application service usage to open source solutions.
D. Define a procurement strategy based on business unit needs.

Answer: D

Explanation:

Upon learning that business units have been independently procuring cloud services, the IT steering committee's best course of action is to define a procurement strategy based on business unit needs. This approach ensures that cloud service procurement aligns with the enterprise's overall IT strategy and governance policies while still addressing the specific requirements of individual business units. It fosters collaboration between IT and business units, ensuring that cloud services are vetted for compliance, security,

and interoperability. Requiring cancellation, including business unit leadership in the EA review board, or limiting usage to open-source solutions may address aspects of the issue but do not provide a comprehensive strategy that aligns business needs with IT governance.

Question: 552

Which of the following would be the BEST way for an enterprise to address new legal and regulatory requirements applicable to IT?

A. Treat as a risk to be assessed before developing a response.
B. Benchmark how other IT organizations are treating the new requirements.
C. Adopt a zero-tolerance approach for noncompliance with regulatory matters.
D. Use a cost-benefit analysis to determine if compliance is warranted.

Answer: A

Explanation:

The best way for an enterprise to address new legal and regulatory requirements applicable to IT is to treat them as a risk to be assessed before developing a response. This approach involves identifying the potential impact of the new requirements on the organization, evaluating the likelihood and consequences of non-compliance, and then developing a prioritized response plan based on this risk assessment. This method ensures a measured and proportional response that aligns with the organization's risk appetite and strategic objectives. While benchmarking, adopting a zero-tolerance approach, and using cost-benefit analysis are useful, they should be part of a broader risk-based strategy to address compliance effectively.

Question: 553

An enterprise is exploring a new business opportunity. Which of the following is the BEST way to help ensure related IT projects deliver the business requirements?

A. Hire a business consultant to manage the projects.
B. Develop a policy to enforce the processes and procedures.
C. Implement stage-gate reviews that require business sign-off.
D. Focus on maturing processes and developing procedures.

Answer: C

Explanation:

To help ensure that IT projects related to a new business opportunity deliver the required business outcomes, the best approach is to implement stage-gate reviews that require business sign-off at each critical phase of the project. This process provides structured checkpoints where project progress, alignment with business requirements, and expected outcomes can be evaluated and validated by business stakeholders. This ensures ongoing alignment between IT project execution and business objectives, allowing for timely adjustments as needed. Hiring consultants, developing policies, and focusing on process maturity are supportive actions, but stage-gate reviews with business sign-off directly link project progression to business expectations.

Question: 554

Which of the following is MOST likely to have a negative impact on accountability for information risk

ownership?

A. The risk owner is a department manager, and the control owner is a member of the risk owner's staff.
B. Information risk is assigned to a department, and an individual owner has not been assigned.
C. The risk owner and the control owner of the information do not work in the same department.
D. The same person is listed as both the control owner and the risk owner for the information.

Answer: B

Explanation:

Assigning information risk to a department without designating an individual owner is most likely to have a negative impact on accountability for information risk ownership. This lack of individual accountability can lead to ambiguities in responsibility, making it difficult to ensure that appropriate risk management actions are taken and followed up on. When an individual owner is clearly identified, it establishes direct responsibility and accountability, improving the effectiveness of risk management practices. While the scenarios described in the other options present challenges, the absence of a specific individual owner represents a fundamental weakness in establishing clear accountability for managing information risk.

Question: 555

Which of the following should a CIO review to obtain a holistic view of IT performance when identifying potential gaps in service delivery?

A. Key performance indicators (KPIs)
B. Return on investment (ROI) analysis
C. Service level agreement (SLA) reporting
D. Staff performance evaluations

Answer: A

Explanation:

To obtain a holistic view of IT performance and identify potential gaps in service delivery, a CIO should review Key Performance Indicators (KPIs). KPIs are quantifiable measures that reflect the critical success factors of an organization and provide a comprehensive overview of performance across various aspects of IT service delivery, including efficiency, effectiveness, quality, and compliance with agreed service levels. While ROI analysis, SLA reporting, and staff performance evaluations offer valuable insights into specific areas, KPIs provide a broader perspective that encompasses various dimensions of IT performance, making them essential for a comprehensive assessment.

Question: 556

Which of the following should be considered FIRST when assessing the implications of new external regulations on IT compliance?

A. IT policies and procedures that need revision
B. Resource burden for implementation
C. Gaps in skills and experience of IT employees
D. Impact on contracts with service providers

Answer: A

Explanation:

When assessing the implications of new external regulations on IT compliance, the first consideration should be the IT policies and procedures that need revision. This initial focus ensures that the foundational guidelines governing IT operations are aligned with the new regulatory requirements, forming the basis for compliance. While the resource burden for implementation, gaps in skills and experience of IT employees, and the impact on contracts with service providers are important considerations, they follow the primary step of ensuring that IT policies and procedures are in compliance with new regulations.

Question: 557

Which of the following is the GREATEST consideration when evaluating whether to comply with the new carbon footprint regulations impacted by blockchain technology?

A. The enterprise's organizational structure
B. The enterprise's risk appetite
C. The current IT process capability maturity
D. The IT strategic plan

Answer: B

Explanation:

The greatest consideration when evaluating whether to comply with new carbon footprint regulations impacted by blockchain technology is the enterprise's risk appetite. This involves understanding the level of risk the organization is willing to accept in relation to the potential environmental impact and regulatory compliance requirements associated with blockchain technology. The organization's risk appetite guides decision-making processes, influencing whether to invest in more sustainable practices or technologies, or to accept the risks associated with noncompliance. While the organizational structure, IT process capability maturity, and the IT strategic plan are relevant, the risk appetite is the key factor in determining the approach to compliance with environmental regulations.

Question: 558

Which of the following is the MOST important consideration regarding IT measures as part of an IT strategic plan?

A. Data collection for the metrics is automated.
B. The metrics can be traced to enterprise goals.
C. Minimum target levels are realistic.
D. Thresholds align to key risk indicators (KRIs).

Answer: B

Explanation:

The most important consideration regarding IT measures as part of an IT strategic plan is that the metrics can be traced to enterprise goals. This alignment ensures that IT initiatives and performance metrics directly contribute to achieving the broader objectives of the organization, demonstrating the value of IT in supporting strategic outcomes. While data collection automation, realistic

minimum target levels, and thresholds aligned to KRIs are important attributes of effective metrics, the ability to trace metrics back to enterprise goals is fundamental to ensuring strategic alignment and justifying IT investments.

Question: 559

An enterprise wants to reduce the complexity of its data assets while ensuring impact to the business is minimized during the transition.
Which of the following should be done FIRST?

A. Remove applications that are not aligned with the information architecture.
B. Review the information classification and retention policies.
C. Review the information architecture.
D. Assess current information ownership.

Answer: C

Explanation:

To reduce the complexity of its data assets while minimizing impact to the business during the transition, an enterprise should first review the information architecture. This review will provide a comprehensive understanding of the current state of data assets, their interdependencies, and how they are managed and utilized within the organization. It forms the basis for identifying redundancies, inefficiencies, and opportunities for simplification. While removing misaligned applications, reviewing classification and retention policies, and assessing information ownership are important, they should be guided by a thorough review of the information architecture to ensure a strategic and effective approach to simplification.

Question: 560

An interna! health organization has been notified that a data breach has resulted in patient records being published online. Which of the
following is MOST important consideration when determining the process for meeting the organization's legal and regulatory obligations?

A. Organizational structure, including accountable partes
B. Data classification and related security policy
C. Context of the breach, including data ownership and location
D. Details of how the breach occurred and related incident response efforts

Answer: C

Explanation:

When determining the process for meeting an internal health organization's legal and regulatory obligations following a data breach, the most important consideration is the context of the breach, including data ownership and location. Understanding who owns the breached data and where it was stored or processed is crucial for determining jurisdictional and regulatory requirements. This context informs the organization's legal obligations, such as notification requirements and potential liabilities. While organizational structure, data classification, security policy, and details of the breach and incident response efforts are relevant, the context of the breach is paramount in guiding the

legal and regulatory response.

Question: 561

Which of the following BEST supports an IT strategy committee's objective to align employee competencies with planned initiatives?

A. Set management goals to hire cooperative work experience students.
B. Specify minimum training hours required for continuing professional education.
C. Require balanced scorecard concepts training of all employees.
D. Add achievement of competencies to employee performance goals.

Answer: D

Explanation:

Adding the achievement of specific competencies to employee performance goals best supports an IT strategy committee's objective to align employee competencies with planned initiatives. This approach directly links employee development and performance evaluation to theacquisition of skills and knowledge required for the organization's strategic initiatives. By embedding competency development into performance goals, employees are incentivized to acquire the necessary skills, ensuring that the workforce is capable of supporting and executing strategic plans. While hiring students, specifying training hours, and requiring balanced scorecard training can contribute to skill development, integrating competency achievement into performance goals ensures a direct and measurable alignment with strategic needs.

Question: 562

Which of the following is a CIO's BEST approach to ensure IT executes against an approved strategy?

A. Ask project management to define the IT activities for accomplishing the strategy.
B. Request IT senior leaders to collectively plan tactics for execution
C. Have IT leaders independently develop goals for their teams.
D. Provide specific direction for execution of the tasks across IT.

Answer: B

Explanation:

The best approach for a CIO to ensure IT executes against an approved strategy is to request IT senior leaders to collectively plan tactics for execution. This collaborative approach leverages the expertise and insights of senior IT leaders to develop a cohesive and aligned plan that supports the strategic objectives. Collective planning fosters ownership and commitment among leaders, ensuring that execution tactics are well-coordinated and aligned with the overall IT strategy. While asking project management to define activities, having leaders independently develop team goals, and providing specific task direction are important, the collective planning by IT senior leaders ensures a strategic and unified approach to execution.

Question: 563

An IT governance committee is reviewing its current risk management policy in light of increased usage of social media within an enterprise. The FIRST task for the governance committee is to:

A. recommend blocking access to social media.
B. review current level of social media usage.
C. initiate an assessment of the impact on the business.
D. reassess the enterprise's bring your own device (BYOD) policy.

Answer: C

Explanation:

When an IT governance committee is reviewing its current risk management policy due to increased usage of social media within an enterprise, the first task should be to initiate an assessment of the impact on the business. This assessment will provide a comprehensive understanding of how social media usage affects various aspects of the business, including productivity, security, data privacy, and compliance with existing policies and regulations. Understanding the business impact will inform the committee's decisions on any necessary policy adjustments or controls to mitigate potential risks associated with social media usage. While reviewing current usage levels, blocking access, and reassessing BYOD policies are relevant considerations, they should be informed by an initial assessment of the business impact to ensure that any actions taken are aligned with the enterprise's strategic objectives and risk tolerance.

Question: 564

When reporting key risk indicators (KRIs) to the board, what information BEST enables risk-based decision-making?

A. Risk appetite, risk threshold, and risk tolerance
B. Classification of current business risk
C. Emerging industry risk trends and benchmarks
D. Costs and resource needs related to risk mitigation measures

Answer: A

Explanation:

Key risk indicators (KRIs) are designed to provide measurable and actionable insights about the risk environment. For the board to make informed risk-based decisions, it is essential to understand the enterprise's risk appetite (what level of risk the organization is willing to take), risk threshold (the limits within which the risks are acceptable), and risk tolerance (the degree of variability the enterprise is willing to endure). These parameters frame the organization's decision-making boundaries and enable the board to align risk responses with strategic objectives. Reference: COBIT 2019 and CGEIT Study Guide.

Question: 565

Which of the following is the FIRST step when developing an IT risk management framework?

A. Promoting a culture of risk awareness
B. Establishing a risk control library
C. Aligning to enterprise risk management (ERM)
D. Establishing risk appetite

Answer: C

Explanation:

Developing an IT risk management framework begins with aligning it to the enterprise risk management (ERM) framework. This ensures consistency across all organizational risk domains and supports the integration of IT risk into the broader enterprise risk strategy. The ERM provides a foundation for identifying, assessing, and managing IT risks in a way that aligns with the organization's overall objectives. Promoting a culture of risk awareness, while critical, is a subsequent step once the framework is defined. Reference: COBIT 2019 Risk Management Process, CGEIT Exam Manual.

Question: 566

Which of the following would be the GREATEST obstacle for effective implementation of an enterprise's information security policy?

A. Corporate culture
B. Threats to corporate information
C. Utilization of cloud-based applications
D. Geographically dispersed staff

Answer: A

Explanation:

Corporate culture is often the greatest challenge to implementing an information security policy effectively. A culture that does not prioritize security, resists change, or lacks awareness about security risks can hinder policy enforcement. While other options such as cloud applications and dispersed staff introduce complexities, a supportive and informed corporate culture is essential to overcoming such obstacles and ensuring policy adherence. Reference: ISACA's Information Security Management principles, CGEIT Review Manual.

Question: 567

From a governance perspective, which of the following functions MUST approve the agreed-upon criteria for a new technology-enabled service before submitting the final high-level design to project stakeholders?

A. Information security
B. Project management office (PMO)
C. Quality assurance (QA)
D. Internal audit

Answer: A

Explanation:

Information security must approve the criteria for technology-enabled services to ensure that all security-related considerations, including compliance, risk mitigation, and data protection, are addressed. This step aligns the service design with the enterprise's security policies and regulatory requirements before it progresses to stakeholders. Other functions such as QA and PMO contribute to execution and oversight, but the responsibility for security approvals rests with information security. Reference: COBIT 2019, ISACA Security Guidance.

Question: 568

An enterprise has decided to adopt cloud services. Which of the following should be established FIRST?

A. Service level agreements (SLAs)
B. Business continuity plan (BCP)
C. Risk tolerance levels
D. Third-party management framework

Answer: C

Explanation:

Before adopting cloud services, it is critical to establish the organization's risk tolerance levels. This ensures that decisions regarding the use of cloud services align with the enterprise's ability and willingness to accept risk, such as data exposure or operational disruptions. Risk tolerance informs the creation of SLAs, third-party

management frameworks, and BCPs, making it a foundational step. Reference: ISACA Cloud Computing Governance guidelines, CGEIT Exam Manual.

Question: 569

Which of the following BEST enables the alignment of user access rights with business requirements?

A. Data classification policy
B. Maturity model
C. System design
D. Data architecture model

Answer: C

Explanation:

The alignment of user access rights with business requirements is most effectively achieved throughsystem design. During the design phase, systems are architected to incorporate role-based access controls, least privilege principles, and segregation of duties based on business needs. While data classification and architecture support information management, and maturity models help assess governance capability,system design operationalizes access controls directly in alignment with enterprise roles and responsibilities. This is supported byCOBIT principlesthat emphasize embedding governance requirements into system design and implementation to ensure alignment, value delivery, and risk mitigation. Reference:
CGEIT Review Manual (based on domain knowledge from Governance of Enterprise IT and COBIT design factors).
COBIT 2019 Design Guide: Aligning Governance System Components.

Question: 570

Which of the following BEST provides an enterprise with greater insight into its environmental, social, and governance (ESG) metrics?

A. Audit committee oversight
B. Benchmarking against similar industries
C. Collaborative tools and approaches
D. Customer satisfaction surveys

Answer: C

Explanation:

Collaborative tools and approachesenable integrated reporting, real-time data collection, and crossfunctional analysis, which are crucial for measuring complex ESG metrics. These tools foster participation from different departments (HR, compliance, sustainability) and ensure that insights are holistic and timely.
While audit oversight provides governance validation and benchmarking offers external comparison,collaborative systems facilitate the ongoing operational visibility needed to manage ESG performance proactively.
Reference:
CGEIT Review Manual guidance on enterprise performance measurement and transparency.
COBIT components: Information flows and culture, ethics, and behavior.
ISACA's insights into ESG integration within IT governance.

Question: 571

Which of the following is the MOST important course of action when initiating a procurement process for a Zero Trust solution?

A. Develop a contracting template for solution procurement.
B. Conduct a thorough assessment of the vendor's security practices.
C. Select an industry-recognized solution used by a benchmarked enterprise.
D. Develop a comprehensive list of required features.

Answer: B

Explanation:

For Zero Trust architecture, which emphasizes "never trust, always verify,"evaluating the vendor's security practices is critical. A thorough security assessment ensures that the vendor aligns with Zero Trust principles, such as identity verification, micro-segmentation, and continuous monitoring.
Although having a feature list and contracting template are important downstream activities, and benchmarking can help shortlist vendors, thecore of Zero Trust lies in trust minimization and verification. Hence, vetting a vendor's capability to enforce security controls is paramount. Reference:
CGEIT Review Manual's risk optimization and resource governance sections.
NIST Zero Trust Architecture guidelines.
COBIT 2019 – Focus Area: Information Security Governance.

Question: 572

The board directed the CIO to ensure that required IT resources are available to execute a new enterprise strategy. Which of the following should be done FIRST to support this initiative?

A. Implement an IT capability strategy
B. Perform a gap analysis
C. Develop a capacity management plan
D. Develop a resource management plan

Answer: B

Explanation:

Performing a gap analysisis the first step in understanding whether existing IT capabilities and resources are sufficient to meet the demands of a new enterprise strategy. A gap analysiscompares current capabilities with the strategic requirements, identifying shortfalls in skills, infrastructure, processes, and other resources. Only after identifying the gaps can appropriate planning (e.g., capacity management, capability strategy, resource management) be effectively initiated.
Reference:
CGEIT Review Manual: Domain 3 – IT Resources: "A gap analysis is a critical first step in strategic alignment, ensuring that resource planning is data-driven and goal-oriented."
COBIT 2019 Focus Area: Enterprise Strategy Alignment and Design Factors.

Question: 573

A newly appointed CIO is concerned that IT is too reactive and wants to ensure IT adds value to the enterprise by proactively anticipating business needs. Which of the following will BEST contribute to meeting this objective?

A. Incorporating IT planning into the enterprise strategic planning process
B. Implementing an IT portfolio management framework
C. Involving more IT representation in strategic business case reviews
D. Including IT management within the program management office

Answer: A

Explanation:

Incorporating IT planning into the enterprise strategic planning processensures that IT initiatives are aligned from the beginning with enterprise goals. This proactive alignment allows IT to anticipate future business needs, allocate resources in advance, and reduce reaction time to strategic shifts. While portfolio management and representation in reviews improve execution and oversight, true proactive value comes fromstrategic integration—ensuring IT is part of the planning conversation rather than reacting post-factum.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT: "Proactive IT governance requires early inclusion in enterprise strategy formulation to ensure that IT is not merely a support function but a strategic enabler."

COBIT 2019 Governance System: Alignment Goals and Governance Objectives.

Question: 574

Which of the following should be done FIRST when developing an IT strategy to support a new AI business strategy?

A. Assess current AI capabilities and infrastructure
B. Establish guidelines and policies for responsible use of AI
C. Create use cases to understand the impact of AI
D. Build a team of AI professionals

Answer: A

Explanation:

Before any strategic direction can be set for AI initiatives,assessing the current AI capabilities and infrastructureis essential. This foundational step provides a baseline of where the organization currently stands, what assets or skills it possesses, and what gaps may exist.

Subsequent actions, such as developing use cases, forming teams, or crafting policies, rely heavily on this understanding. Without a proper assessment, strategic decisions may be misaligned with the organization's actual readiness or capabilities.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources and Strategic Alignment: "Assessment of currentstate capabilities is a prerequisite for any IT strategic development effort."

COBIT 2019 Design Guide: "Define and analyze the current state before building the target state roadmap."

Question: 575

When determining the desired maturity levels for IT governance processes, it is MOST important to:

A. Focus on existing strengths as key drivers for the target levels
B. Ensure target levels are in line with external competitor benchmarks
C. Agree on target levels in response to need
D. Ensure that maturity can be achieved at the lowest cost

Answer: C

Explanation:

The correct approach is toagree on target maturity levels in response to need—this ensures that the maturity level supports enterprise objectives, risk appetite, and strategic priorities. The maturity should be fit-for-purpose, rather than arbitrarily benchmarked or driven solely by cost or strengths. While competitor

benchmarks and cost considerations can provide insight, they are secondary to ensuring that the governance processes meetspecific business and governance needs.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT: "Target capability levels should be based on enterprise strategy, goals, and risk appetite, and not only on industry averages or cost." COBIT 2019 Design Guide: Tailoring Governance System Design – "Target capability levels should be derived from governance and management objectives prioritized based on enterprise needs."

Question: 576

Which of the following situations provides the BEST justification for considering the adoption of a qualitative risk assessment method?

A. Determining a quantitative risk score would require complex calculations
B. It is cost prohibitive to obtain relevant historical quantitative data
C. There are fewer information assets in the risk register
D. A higher risk tolerance level has been defined by enterprise leadership

Answer: B

Explanation:

Qualitative risk assessmentis most appropriate when reliable quantitative data is unavailable or too costly to gather. In such cases, qualitative methods (like risk matrices or expert judgment) provide valuable input based on impact and likelihood without requiring precise numerical data.

This approach is especially useful in new or evolving domains (e.g., cybersecurity or AI) where historical data may be lacking.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization: "Qualitative assessments are suitable when quantitative methods are not feasible due to lack of historical data or high costs associated with obtaining it."

COBIT 2019 Focus Area: Risk Management.

Question: 577

The board of an organization has been informed of possible cyberthreats. Which of the following should be the board's NEXT course of action?

A. Evaluate the security incident response process
B. Reevaluate the risk tolerance of the organization
C. Ask the CIO to report on a risk response
D. Engage the CIO to evaluate the risk

Answer: D

Explanation:

The board's role isoversight, not direct execution. Upon learning of cyberthreats, the appropriate governance response is toengage executive leadership (e.g., the CIO) to evaluate the riskand report back with an impact assessment and potential responses.

This enables the board to make informed decisions and ensures the matter is handled within the appropriate executive management structure.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT: "Boards should assign evaluation and reporting

responsibilities to management while ensuring accountability is maintained at the executive level."
COBIT 2019: Governance Objective EDM03 (Ensure Risk Optimization) – emphasizes delegation and structured risk evaluation by executives.

Question: 578

When developing IT risk management policies and standards, it is MOST important to align them with:

A. The corporate risk culture
B. The enterprise risk management (ERM) framework
C. Enterprise goals and objectives
D. Best practices for IT risk management

Answer: B

Explanation:

Alignment with the enterprise risk management (ERM) frameworkis the top priority when developing IT risk management policies. This ensures that IT risk is not managed in a silo but is integrated into the broader enterprise risk posture, decision-making processes, and governance. While corporate culture and best practices are influential, and goals and objectives shape
strategy,only the ERM framework provides the structured foundation for aligning IT risk with enterprise-wide risk management.

Reference:
CGEIT Review Manual: Domain 4 – Risk Optimization: "IT risk management must be aligned with the enterprise's risk management framework to ensure consistent practices, shared language, and coordinated responses."
COBIT 2019: APO12 (Manage Risk).

Question: 579

Executive management is concerned that IT has not achieved its performance targets. At the end of the fiscal year, it was noted the reason was largely due to insufficient spending on key IT initiatives. Which of the following would help to alleviate the issue for the coming year?

A. Key risk indicators (KRIs)
B. Stage gate reviews
C. Lag indicators
D. Lead indicators

Answer: D

Explanation:

Lead indicatorsare proactive metrics that provide early signals of performance, enabling timely action before outcomes are realized. In this case, insufficient investment led to missed targets—a lead indicator could help forecast spending trends or progress toward milestones before year-end. Lag indicators (e.g., annual performance) show outcomes after the fact. KRIs and stage gates are valuable but are not direct predictors of performance outcomes related to investment levels. Reference:
CGEIT Review Manual: Domain 3 – Benefits Realization: "Lead indicators are essential for performance forecasting and timely intervention."
COBIT 2019: BAI09 (Manage Performance and Capacity).

Question: 580

Which of the following is the BEST way to express the value of financial investments in cybersecurity?

A. Payback period
B. Cost-benefit analysis
C. Net present value (NPV)
D. Internal rate of return (IRR)

Answer: B

Explanation:

Cost-benefit analysisis the most effective and practical approach for evaluating the value of cybersecurity investments. It allows comparison of expected benefits (risk reduction, incident cost avoidance, compliance) against the costs (investment, operations).

While NPV and IRR are solid financial tools, they are better suited to revenue-generating projects.

Cybersecurity's value is often intangible or indirect, making a straightforwardcost-benefit frameworkmore suitable.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization and Business Case Justification COBIT 2019: EDM02 (Ensure Benefits Delivery).

Question: 581

An enterprise has launched a digitization effort requiring a single view of customer information across all product lines. Which of the following should be done FIRST to enable this initiative?

A. Develop funding estimates for integrating applications
B. Modify the future state enterprise architecture (EA)
C. Assess the current data standards that are in use for applications
D. Audit the infrastructure architecture for integration points

Answer: C

Explanation:

The foundational step in achieving a single customer view is toassess the current data standardsused across applications. Without understanding data definitions, structures, and inconsistencies, any integration or architectural modification would be premature and potentially misaligned.

Future-state planning and funding depend on a clear grasp of the current data landscape and challenges.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources (Data Management)

COBIT 2019: DSS06 (Manage Business Process Controls).

Question: 582

Which of the following should be the PRIMARY consideration when developing an IT strategy for the global implementation of Internet of Things (IoT) solutions?

A. Hiring additional IT staff with IoT expertise
B. Addressing security and privacy
C. Identifying cost-effective IoT devices
D. Maintaining compatibility with legacy systems

Answer: B

Explanation:

Security and privacyare paramount when implementing IoT on a global scale. IoT devices often introduce vulnerabilities and handle sensitive data across diverse jurisdictions, making security controls and privacy compliance essential from the outset.

While staffing, cost, and integration are important,security and privacyrepresent the greatest strategic and reputational risk if not addressed early in the strategy.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization

COBIT 2019: DSS05 (Manage Security Services) and APO13 (Manage Security).

Question: 583

Which of the following is the BEST way to minimize the potential mishandling of customer personal information in a system that is located in a country with strict privacy regulations?

A. Revise IT policies, standards, and procedures
B. Implement a SIEM solution
C. Consult the legal and compliance department
D. Establish new IT key risk indicators (KRIs)

Answer: C

Explanation:

When operating in a jurisdiction withstrict privacy regulations, the first and most effective step is toconsult the legal and compliance department. They can provide guidance to ensure full compliance with local laws, such as GDPR or other data protection mandates, reducing the risk of regulatory noncompliance.

While revising policies or implementing technical controls (e.g., SIEM, KRIs) is useful, legal compliance is foundational and dictates how other controls should be shaped.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization and Compliance

COBIT 2019: DSS01 (Manage Operations) and EDM01 (Ensure Governance Framework Setting and Maintenance).

Question: 584

Which of the following is MOST important to ensure when aligning IT and enterprise resource management processes?

A. IT sourcing processes are in place
B. IT provides input for business strategy development
C. IT resources are mapped to business priorities
D. IT resource monitoring and oversight is in place

Answer: C

Explanation:

Themost critical factor in aligning IT and enterprise resource managementis ensuring thatIT resources are mapped to business priorities. This guarantees that resource allocation supports strategic objectives and delivers maximum value.

Without this alignment, IT efforts may be misdirected, underutilized, or not supporting enterprise goals—even if sourcing and monitoring are in place.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources

COBIT 2019: APO07 (Manage Human Resources), BAI01 (Manage Programs and Projects).

Question: 585

A CIO engages a consulting firm to conduct a benchmark analysis of the organization's IT governance framework against industry best practices. Several recommendations to improve the maturity of the framework are identified. Which of the following should be the CIO's NEXT course of action?

A. Develop a plan to integrate the recommendations
B. Appoint a project manager to implement the recommendations
C. Obtain approval from the IT steering committee to implement the recommendations
D. Evaluate the feasibility of the recommendations

Answer: D

Explanation:

After receiving recommendations, thefirst logical step is to evaluate the feasibility—this includes assessing alignment with strategic goals, resource availability, risk tolerance, and operational impact. Implementing or planning without a feasibility assessment may result in impractical or misaligned actions.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT

COBIT 2019: EDM02 (Ensure Benefits Delivery), APO02 (Manage Strategy).

Question: 586

A global organization has noticed a significant decrease in the return on IT investments in a particular region. To enhance project governance in this region, the CEO should FIRST

A. Perform a program benefit calculation and review the project selection methodology
B. Suspend funding until project managers from better-performing regions can be assigned
C. Perform an independent review of business cases for each current and proposed project in the region
D. Work with the region's leadership to better understand why the situation has occurred

Answer: D

Explanation:

Understanding the root causeis the essential first step. The CEO shouldwork with regional leadershipto gather context before applying solutions or imposing changes. This collaborative approach ensures that corrective actions are informed, targeted, and not based on assumptions. Other steps like reviewing business cases or revising benefits calculations may follow, butdiagnosis must come before treatment.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization

COBIT 2019: EDM04 (Ensure Resource Optimization).

Question: 587

A board of directors has mandated that key performance indicators (KPIs) be developed for all IT projects that are created in support of a business objective. Which of the following MUST be reflected in the KPIs to be effective?

A. Future-state architecture
B. Critical success factors (CSFs)
C. Portfolio management principles
D. Key risk indicators (KRIs)

Answer: B

Explanation:

Critical success factors (CSFs)are the specific conditions or variables that are essential for achieving business objectives. Effective KPIs must align with these CSFs to ensure they measure what truly matters to project and business success.

KRIs relate to risk, and while important, they serve a different purpose. Future-state architecture and portfolio principles guide strategy, butCSFs provide the foundational context for performance measurement.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization and Performance Measurement

COBIT 2019: BAI01 (Manage Programs and Projects), MEA01 (Monitor, Evaluate and Assess Performance and Conformance).

Question: 588

An ongoing project is on track according to project plan. However, a recent regulation change will have a major impact to the project. The project sponsor's NEXT step should be to:

A. Seek exemption from the appropriate regulatory body
B. Perform an impact analysis and update the business case
C. Submit the project to the IT steering committee for reapproval
D. Rescope the project to remove work impacted by the regulation

Answer: B

Explanation:

When a regulatory change significantly affects an ongoing project, thefirst step should be to perform an impact analysis and update the business case.This helps the organization understand how the change influences cost, timelines, compliance, and value delivery.

Only after understanding the impact should actions such as seeking reapproval, changing scope, or applying for exemptions be considered. This aligns with the principle of informed decision-making in IT governance.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization, Change Management

COBIT 2019: BAI01 (Manage Programs and Projects), EDM02 (Ensure Benefits Delivery).

Question: 589

An enterprise recently experienced a major breach that was escalated effectively. However, the recovery took far longer than expected, resulting in significant financial loss. Which of the following is MOST likely the root cause of this scenario?

A. Key performance indicators (KPIs) were not regularly monitored
B. The recovery point objective (RPO) was not established
C. The disaster recovery plan (DRP) was not routinely updated
D. The business continuity plan (BCP) was not recently tested

Answer: D

Explanation:

The most likely root cause in this scenario is that thebusiness continuity plan (BCP) was not recently tested.A plan may exist and be theoretically sound, but without testing, organizations cannot assess whether recovery procedures work effectively under real conditions.

Testing ensures that time estimates are realistic, personnel understand their roles, and systems perform as expected. A lack of testing results in delays, confusion, and extended recovery times— even with escalation processes functioning well.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization, Continuity Management

COBIT 2019: DSS04 (Manage Continuity).

Question: 590

Which of the following BEST enables an enterprise to determine an appropriate retention policy for its information assets?

A. Business and compliance requirements
B. Business storage and processing needs
C. Backup and restoration capabilities
D. External customer data retention requirements

Answer: A

Explanation:

An effective information retention policy must be based onbusiness and compliance requirements.These include legal mandates, industry regulations, and internal operational needs that dictate how long data must be retained and when it should be archived or deleted.

While storage needs, backups, or customer expectations matter,only regulatory and business alignment guarantees legal compliance and operational relevance.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources (Data Governance)

COBIT 2019: DSS01 (Manage Operations), DSS06 (Manage Business Process Controls).

Question: 591

An enterprise is concerned about the community impact of its data center noise levels. Which of the following is the enterprise's BEST course of action?

A. Proactively reduce after-hours operations
B. Pursue acquisition of surrounding properties
C. Wait for a formal complaint to be filed
D. Seek input from appropriate stakeholders

Answer: D

Explanation:

Thebest governance-aligned approachis toseek input from appropriate stakeholders, including community representatives, environmental groups, and local government. This enables the organization to address concerns proactively and collaboratively, minimizing reputational and regulatory risks.

Waiting for complaints or making unilateral decisions (like buying land or reducing hours) may be less effective or even inappropriate without stakeholder input.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT, Stakeholder Engagement COBIT 2019: EDM05 (Ensure Stakeholder Engagement).

Question: 592

The PRIMARY objective of establishing outcome measures is to:

A. Clarify the cause-and-effect relationship of the strategy
B. Monitor whether the chosen strategy is successful
C. Understand how the strategy will be achieved
D. Demonstrate commitment to IT governance

Answer: B

Explanation:

Theprimary objective of outcome measuresis tomonitor whether the strategy is achieving its intended results. These measures evaluate the effectiveness and impact of the strategy after implementation, helping guide course corrections and value realization.

While clarifying strategy and governance are important,outcome measures are specifically about tracking success and performance results.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization and Performance Measurement
COBIT 2019: MEA01 (Monitor, Evaluate and Assess Performance and Conformance).

Question: 593

Which of the following BEST enables an enterprise to minimize the risks of intellectual property theft and loss of sensitive information when acquiring Internet of Things (IoT) hardware and software components?

A. Review the data classification policy and relevant documentation
B. Terminate contracts with suppliers from sanctioned regions of the world
C. Require nondisclosure agreements (NDAs) from all suppliers
D. Integrate supply chain cyber risk management processes

Answer: D

Explanation:

The best way to minimize intellectual property theft and sensitive information loss in IoT acquisitions is to integrate supply chain cyber risk management processes. This holistic approachincludes assessing supplier security posture, monitoring for threats, and ensuring cybersecurity is embedded into procurement, delivery, and operations.

NDAs, sanctions, and data classification are supportive, but only supply chain risk management addresses the full lifecycle risks and modern threats in globally sourced IoT ecosystems.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization

COBIT 2019: DSS05 (Manage Security Services), APO10 (Manage Suppliers).

Question: 594

Which of the following presents the GREATEST challenge for a large-scale enterprise when procuring Infrastructure as a Service (IaaS)?

A. Testing the vendor resiliency plan annually
B. Protecting the enterprise from labor liability
C. Ensuring the vendor meets corporate requirements
D. Monitoring key performance indicators (KPIs)

Answer: C

Explanation:

For large enterprises, the greatest challenge when procuring IaaS is ensuring the vendor meets corporate requirements, including compliance, integration standards, security, scalability, and service levels. The complexity of aligning cloud capabilities with internal policies and operational needs can create governance gaps.

Other options represent necessary practices, but the alignment of vendor capabilities with enterprise standards is foundational to long-term success and risk mitigation.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources and Third-Party Risk

COBIT 2019: APO03 (Manage Enterprise Architecture), APO10 (Manage Suppliers).

Question: 595

Business management is seeking assurance from the CIO that IT has a plan in place for early identification of potential issues that could impact the delivery of a new application. Which of the following is the BEST way to increase the chances of a successful delivery?

A. Implement a release and deployment plan
B. Ask the application owner to update the risk register
C. Create a baseline configuration of the new application
D. Perform user acceptance testing (UAT)

Answer: A

Explanation:

A release and deployment plan outlines structured activities to transition new applications into production. It includes monitoring, testing, fallback procedures, and risk identification mechanisms— helping identify and address potential issues early.

While UAT and risk updates are helpful, and configurations ensure consistency, a formal release and deployment plan is the most comprehensive tool for early issue detection and delivery assurance.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization

COBIT 2019: BAI07 (Manage Change Acceptance and Transitioning).

Question: 596

Which of the following is the GREATEST driver of ethical decision making in an IT enterprise?

A. Corporate culture
B. Process and control environment
C. Code of conduct
D. Training and awareness programs

Answer: A

Explanation:

Corporate culture is the most influential driver of ethical decision-making. It shapes the behavior, attitudes, and values of individuals and determines whether ethical frameworks like codes of conduct and training programs are truly effective in practice.

While control environments and training reinforce behavior, the culture sets the tone from the top, influencing whether ethics are embraced or bypassed.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT

COBIT 2019: Governance System Component – Culture, Ethics and Behavior.

Question: 597

Which of the following should be the MOST important consideration when establishing key performance indicators (KPIs) for IT initiatives?

A. An owner can be assigned
B. Processes can be optimized
C. Data collection can be automated
D. Quality has been evaluated

Answer: D

Explanation:

The quality of KPIs is the most important consideration. KPIs must be relevant, accurate, aligned with objectives, and capable of driving meaningful decision-making. Without quality evaluation, even automated or well-owned KPIs may mislead or fail to reflect performance accurately.

Assignment and automation enhance implementation, but they do not ensure the KPI's value or appropriateness for measuring success.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization and Performance Monitoring

COBIT 2019: MEA01 (Monitor, Evaluate and Assess Performance and Conformance).

Question: 598

When an enterprise outsources to a third-party data center, who is accountable for the governance of data retention controls for the data that has been transferred?

A. The enterprise's internal audit team
B. The third party's data steward
C. The third party's control operators
D. The enterprise's data owner

Answer: D

Explanation:

The enterprise's data owner retains accountabilityfor the governance of data retention, even when the data is transferred to a third party. Outsourcing does not eliminate governance responsibilities; the data owner must ensure compliance with policies, regulations, and contractual terms, including how long data is retained and under what conditions.

While third parties execute controls,the enterprise remains accountable for the data and its governance outcomes.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources, Data Governance

COBIT 2019: DSS01 (Manage Operations), APO10 (Manage Suppliers).

Question: 599

Which of the following is the BEST indicator for measuring performance when implementing DevSecOps in an enterprise?

A. Mean time to repair
B. Percentage of automated tests
C. Deployments per day
D. Number of defects released per day

Answer: B

Explanation:

Percentage of automated testsis a key indicator in DevSecOps because it reflects the integration of security and quality into the development lifecycle. Automation is a cornerstone of DevSecOps, enabling continuous integration and deployment with embedded testing and security validation. While mean time to repair and deployment frequency are valuable,automation directly supports the goals of security, speed, and reliability in DevSecOps.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization

COBIT 2019: BAI03 (Manage Solutions Identification and Build), DSS05 (Manage Security Services).

Question: 600

Following a recent change to enterprise strategy, which of the following would be MOST important for the CIO to review?

A. Existing performance and capacity plans
B. A list of current and planned IT projects
C. Historical IT budget allocations
D. The enterprise SWOT analysis

Answer: B

Explanation:

When enterprise strategy changes, themost important action for the CIO is to review the portfolio of current and planned IT projectsto ensure alignment with the new strategic direction. This ensures that resources are being allocated to initiatives that support updated goals and that outdated or misaligned projects are reevaluated.

Performance plans and historical budgets offer context butdo not directly enable strategic realignment.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT, Strategic Alignment

COBIT 2019: APO02 (Manage Strategy), BAI01 (Manage Programs and Projects).

Question: 601

An enterprise has decided to invest in Internet of Things (IoT) technology as part of its strategic plan. Which of the following presents the GREATEST risk to consider as part of the technical risk management process?

A. Device vulnerabilities
B. Technology integration
C. Device performance
D. Technology obsolescence

Answer: A

Explanation:

Device vulnerabilitiesrepresent the greatest technical risk in IoT implementations. IoT devices often have limited security features, can be difficult to patch, and may be deployed in large numbers— making them a common attack vector.

Integration and obsolescence matter, butvulnerabilities directly impact data protection, system integrity, and compliance, posing an immediate and high-priority risk.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization

COBIT 2019: DSS05 (Manage Security Services), APO12 (Manage Risk).

Question: 602

As a result of a new regulatory requirement, an enterprise's board has mandated that steps be taken to ensure related IT governance activities are performing as originally designed and are continuously improved. Which of the following is the BEST approach?

A. Mandate ongoing enterprise risk and control self-assessments (CSAs)
B. Conduct quarterly reviews of the enterprise business architecture
C. Engage periodic external audit reviews of IT governance processes
D. Require annual mapping of key IT governance processes

Answer: A

Explanation:

Control self-assessments (CSAs)are the best method to continuously monitor and improve IT governance activities. CSAs empower internal teams to regularly evaluate performance, identify gaps, and initiate corrective actions, ensuring ongoing compliance and alignment with governance objectives.

External audits and mappings are periodic and less dynamic, whereasCSAs offer proactive, continuous oversight.

Reference:

CGEIT Review Manual: Domain 1 – Governance of Enterprise IT, Performance Measurement COBIT 2019: MEA02 (Monitor, Evaluate and Assess the System of Internal Control).

Question: 603

An enterprise's current business continuity plan (BCP) fails to consider many common crisis events. What would be MOST helpful to address this situation?

A. Engage stakeholders in scenario development
B. Review the root cause analysis
C. Require further walk-through tests
D. Review and update the crisis communication plan

Answer: A

Explanation:

Engaging stakeholders in scenario developmentis essential to identifying relevant and realistic crisis events that the business continuity plan should address. Stakeholders bring diverse perspectives on potential threats and operational priorities, which improves the completeness and effectiveness of the BCP.

Walk-throughs and communication reviews are important later stages, butscenario development is foundationalfor making the BCP comprehensive.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization

COBIT 2019: DSS04 (Manage Continuity).

Question: 604

An enterprise is evaluating both a virtual reality (VR) project and an augmented reality (AR) project. Which of the following should be the MOST important objective when evaluating these two projects within IT portfolio management?

A. Maximizing the earned value of IT investments
B. Determining which IT project to discontinue
C. Implementing efficient and effective solutions
D. Reducing the risk exposure of the projects

Answer: A

Explanation:

Within IT portfolio management, themost important objective is maximizing the earned value of IT investments.This ensures that projects contribute meaningfully to enterprise goals, provide strong return on investment, and optimize the use of limited IT resources.

Decisions about discontinuation or risk are part of the process, butvalue delivery is the primary metricin portfolio optimization.

Reference:
CGEIT Review Manual: Domain 3 – Benefits Realization
COBIT 2019: EDM02 (Ensure Benefits Delivery), APO05 (Manage Portfolio).

Question: 605

An audit department recently uncovered a series of security breaches. It was determined that network intrusion detection logs were recording the suspicious activity, but IT staff were not reviewing logs due to competing business demands. To address this situation, the IT steering committee's FIRST priority should be:

A. A re-prioritization of IT projects to address critical needs
B. Updating the RACI chart to establish responsibility
C. The hiring of additional staff to cope with the demand
D. An assessment of the capacity of current resources

Answer: A

Explanation:

Given that critical security monitoring was being neglected due to other demands, theIT steering committee's first priority should be to re-prioritize IT projects.This ensures that resources are allocated to security monitoring and risk mitigation, which are essential to enterprise protection. Assessments and staffing changes may follow, butthe immediate governance action is to adjust prioritiesin light of organizational risk.

Reference:
CGEIT Review Manual: Domain 4 – Risk Optimization
COBIT 2019: APO01 (Manage the IT Management Framework), APO12 (Manage Risk).

Question: 606

Which of the following is MOST relevant to report to the board of directors regarding the execution of IT strategy?

A. Service level agreements (SLAs) for outsourced IT initiatives
B. Total IT spend from all current IT initiatives
C. Realization of benefits in the business case
D. IT strategy risk metrics related to critical services and projects

Answer: C

Explanation:

Boards are most concerned with whether IT investments aredelivering the expected value and business outcomes. Thus, therealization of benefits in the business caseis the most relevant indicator of IT strategy execution effectiveness.

Risk metrics, SLAs, and spending detail are important butdo not directly measure success in achieving strategic outcomes.

Reference:
CGEIT Review Manual: Domain 3 – Benefits Realization COBIT 2019: EDM02 (Ensure Benefits Delivery).

Question: 607

An enterprise's board of directors is concerned about the ongoing costs of a large inventory of Internet of

Things (IoT) devices. Which of the following should the CIO do FIRST?

A. Implement performance measures for each IoT device
B. Suggest replacing IoT devices that are too expensive
C. Assess the benefits of IoT capabilities
D. Reduce the budget for IoT capability to meet stakeholder expectations

Answer: C

Explanation:

Before taking cost-cutting actions, theCIO should assess the benefits of IoT capabilitiesto understand whether the investments are delivering value. This evaluation provides the context needed to justify current costs or to make informed decisions about optimization.

Jumping to budget cuts or replacements without understanding valuecould undermine strategic benefits.

Reference:

CGEIT Review Manual: Domain 3 – Benefits Realization

COBIT 2019: EDM02 (Ensure Benefits Delivery), APO06 (Manage Budget and Costs).

Question: 608

When an enterprise plans to deploy mobile device technologies, it is MOST important for leadership to ensure that:

A. Users agree to an acceptable use policy
B. Appropriate controls are implemented
C. The IT policy addresses mobile devices
D. The project management office (PMO) is engaged

Answer: B

Explanation:

Implementing appropriate controlsis the most critical leadership responsibility when deploying mobile technologies. Controls cover access, encryption, monitoring, and loss prevention— addressing core risks such as data leakage and unauthorized access.

Acceptable use and policy alignment are necessary, butcontrols ensure security and compliance in practice.

Reference:

CGEIT Review Manual: Domain 4 – Risk Optimization

COBIT 2019: DSS05 (Manage Security Services), APO13 (Manage Security).

Question: 609

A CIO observes that many information assets are hosted on legacy technology that can no longer be patched or updated. The systems are not currently in use, but business units are reluctant to decommission assets due to information retention requirements. Which of the following is the BEST strategic response to this situation?

A. Ensure the legacy systems are behind a secure firewall
B. Isolate the legacy systems and disconnect them from the internet
C. Apply legacy system surcharges to the business units
D. Develop and enforce life cycle policies in consultation with business

Answer: D

Explanation:

Thebest strategic responseis todevelop and enforce IT asset life cycle policies in consultation with business units. This approach ensures that legacy systems are managed proactively and collaboratively, balancing risk management, regulatory compliance, and operational needs. Policies should define criteria for decommissioning, archival solutions, and acceptable retention practices. Firewalls and isolation are tactical mitigations, not strategic solutions. Surcharges may discourage usage but do not resolve governance and retention challenges comprehensively.

Reference:

CGEIT Review Manual: Domain 2 – IT Resources (IT Asset Management and Life Cycle) COBIT 2019: BAI09 (Manage Assets), APO01 (Manage the IT Management Framework).

Question: 610

An IT value delivery framework PRIMARILY helps an enterprise:

A. Improve value of successful IT projects.
B. Increase transparency of value to the enterprise.
C. Assist top management in approving IT projects.
D. Optimize value to the enterprise.

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Benefits Realization domain, emphasizes ensuring that IT investments deliver maximum value aligned with business objectives. An IT value delivery framework is a structured approach to managing IT initiatives to ensure they create, sustain, and optimize value for the enterprise. This involves defining value metrics, aligning IT projects with strategic goals, and monitoring outcomes throughout the project lifecycle.

Option D: Optimize value to the enterprise is the primary purpose of an IT value delivery framework. The framework ensures that IT investments are prioritized, executed, and evaluated to maximize benefits (e.g., revenue growth, cost savings, operational efficiency) while minimizing risks and costs. For example, it might use value management techniques (e.g., cost-benefit analysis, ROI tracking) to ensure IT projects deliver measurable outcomes aligned with enterprise goals. The manual likely references COBIT 2019's APO05-Managed Portfolio, which focuses on optimizing the value of IT investments.

Option A: Improve value of successful IT projects is too narrow, as the framework aims to optimize value across all IT initiatives, not just successful ones.

Option B: Increase transparency of value to the enterprise is a secondary benefit. While transparency (e.g., through reporting) is important, the primary goal is value optimization.

Option C: Assist top management in approving IT projects is a governance function, not the primary focus of value delivery, which occurs post-approval during execution and evaluation.

Double Verification: The answer aligns with COBIT's APO05 and the CGEIT domain's focus on benefits realization. The term "optimize value" is consistent with ISACA's emphasis on maximizing stakeholder value in GEIT.

ISACA CGEIT Review Manual 8th Edition, Domain 3: Benefits Realization (focus on value management).

COBIT 2019, APO05-Managed Portfolio.

ISACA Glossary (for definitions of value delivery), available at https://www.isaca.org/resources/glossary.

Question: 611

Which of the following is the GREATEST benefit of using the life cycle approach to govern information assets?

A. Information availability is improved.
B. Operational costs are maintained.
C. Compliance with regulatory requirements is ensured.
D. Overall costs are optimized.

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, covers the governance of information assets, including their management across the entire lifecycle (creation, storage, use, archival, disposal). A life cycle approach ensures that information assets are managed systematically to align with business needs, reduce risks, and optimize resources.

Option D: Overall costs are optimized is the greatest benefit. By governing information assets through their lifecycle, enterprises can minimize costs associated with storage, maintenance, and compliance (e.g., avoiding penalties for improper data retention). For example, the approach identifies redundant data for deletion, optimizes storage solutions, and ensures cost-effective compliance with regulations. The manual likely references COBIT 2019's BAI09-Managed Assets, which emphasizes lifecycle management to achieve cost efficiency.

Option A: Information availability is improved is a benefit, but it's not the greatest, as availability is just one aspect of governance (e.g., via access controls).

Option B: Operational costs are maintained is inaccurate, as the goal is to reduce, not merely maintain, costs.

Option C: Compliance with regulatory requirements is ensured is a significant benefit, but cost optimization encompasses compliance (e.g., avoiding fines) and other savings, making it broader. Double Verification: The answer aligns with COBIT's focus on asset management and the CGEIT domain's emphasis on cost-effective governance. Cost optimization is a recurring theme in ISACA's frameworks for lifecycle management.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on information asset management).

COBIT 2019, BAI09-Managed Assets.

ISACA Glossary (for definitions of lifecycle management), available at https://www.isaca.org/resources/glossary.

Question: 612

Which of the following is the BEST way to help ensure that IT human resources are skilled and available?

A. Focus on outsourcing as an option for supplementing IT human resources.
B. Integrate IT training requests with IT budget planning.
C. Align IT human resource (HR) management processes with internal training.
D. Align IT human resource (HR) management with business planning.

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its IT Resources domain, addresses the management of IT human

resources to ensure they have the skills and availability to support enterprise objectives. Aligning IT HR management with business needs ensures that staffing, skills development, and resource allocation are driven by strategic priorities.

Option D: Align IT human resource (HR) management with business planning is the best approach. This ensures that IT HR strategies (e.g., hiring, training, retention) are directly tied to the enterprise's business goals, such as digital transformation or new service launches. For example, if the business plans to adopt cloud technologies, HR can prioritize hiring cloud architects or training existing staff. The manual likely references COBIT 2019's APO07-Managed Human Resources, which emphasizes aligning IT HR with business strategies.

Option A: Focus on outsourcing is a tactical solution, not a comprehensive strategy, and may not address internal skill development.

Option B: Integrate IT training requests with IT budget planning is important but narrower, focusing only on training funding rather than overall HR alignment.

Option C: Align IT HR management processes with internal training is limited to training and doesn't address broader HR needs like recruitment or capacity planning.

Double Verification: The answer aligns with COBIT's APO07 and the CGEIT domain's focus on strategic resource management. Business alignment is a core principle in ISACA's HR management guidance.

ISACA CGEIT Review Manual 8th Edition, Domain 2: IT Resources (focus on human resource management).
COBIT 2019, APO07-Managed Human Resources.
ISACA Glossary (for definitions of HR management), available at https://www.isaca.org/resources/glossary.

Question: 613

Which of the following is the BEST way for an IT steering committee to determine the benefits of an IT investment?

A. Measure return on investment (ROI) during implementation.
B. Measure net present value (NPV) during stage gate review.
C. Measure planned versus actual spend on the project.
D. Measure value creation throughout the economic life cycle.

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Benefits Realization domain, stresses the importance of evaluating IT investments to ensure they deliver sustained value to the enterprise. The IT steering committee needs a holistic approach to assess benefits, not just financial metrics at specific points. Option D: Measure value creation throughout the economic life cycle is the best approach. This involves tracking benefits (e.g., revenue growth, cost savings, customer satisfaction) from project initiation through implementation and into ongoing operations, ensuring the investment delivers value over its full lifecycle. For example, a new CRM system's benefits (e.g., improved sales) should be measured post-implementation to confirm sustained value. The manual likely references COBIT 2019's APO05-Managed Portfolio, which advocates for lifecycle-based value management. Option A: Measure ROI during implementation is premature, as ROI is most meaningful post-implementation when benefits are realized.

Option B: Measure NPV during stage gate review is useful for decision-making but focuses on financial projections at a single point, not actual benefits.

Option C: Measure planned versus actual spend tracks costs, not benefits, and is irrelevant to value creation.

Double Verification: The answer aligns with COBIT's emphasis on lifecycle value management and the CGEIT

domain's focus on benefits realization. Lifecycle measurement is a standard ISACA practice for IT investments.

ISACA CGEIT Review Manual 8th Edition, Domain 3: Benefits Realization (focus on value measurement).
COBIT 2019, APO05-Managed Portfolio.
ISACA Glossary (for definitions of value creation), available at https://www.isaca.org/resources/glossary.

Question: 614

An enterprise is required to implement several regulatory requirements. Which of the following functions is BEST suited to determine compliance priorities?

A. Legal counsel
B. The IT risk department
C. The audit department
D. Business units

Answer: A

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, addresses compliance with regulatory requirements as a key governance responsibility. Determining compliance priorities involves understanding legal obligations, assessing their impact, and aligning them with business objectives.
Option A: Legal counsel is best suited to determine compliance priorities. Legal counsel has the expertise to interpret regulatory requirements, assess their applicability, and prioritize them based on legal risks, penalties, and business impact. For example, they can identify which regulations (e.g., GDPR, HIPAA) pose the greatest risk of fines or reputational damage and recommend prioritization. The manual likely references COBIT 2019's MEA01-Monitor, Evaluate, and Assess Performance and Conformance, which includes legal compliance as a governance responsibility.
Option B: The IT risk department focuses on IT-specific risks, not broader regulatory compliance, and lacks legal expertise.
Option C: The audit department evaluates compliance post-implementation but isn't responsible for prioritizing regulatory requirements.
Option D: Business units are stakeholders but lack the legal knowledge to prioritize regulations effectively.
Double Verification: The answer aligns with COBIT's governance processes and the CGEIT domain's emphasis on compliance management. Legal counsel's role in regulatory interpretation is a standard practice in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on compliance management).
COBIT 2019, MEA01-Monitor, Evaluate, and Assess Performance and Conformance.
ISACA Glossary (for definitions of compliance), available at https://www.isaca.org/resources/glossary.

Question: 615

Which of the following is the PRIMARY objective of quantum computing architecture when addressing complex problems in a short amount of time using specialized algorithms?

A. To increase revenue
B. To optimize efficiency
C. To reduce cyberattacks
D. To minimize operating costs

Answer: B

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Strategic Management domain, addresses the alignment of IT strategies with emerging technologies to support enterprise objectives. Quantum computing architecture is designed to solve complex problems (e.g., optimization, cryptography, simulations) faster than classical computing by leveraging quantum algorithms. The manual would likely discuss the strategic adoption of such technologies to enhance computational efficiency.
Option B: To optimize efficiency is the primary objective. Quantum computing excels at solving specific problems (e.g., combinatorial optimization, molecular modeling) with specialized algorithms (e.g., Grover's, Shor's) that significantly reduce computation time compared to classical systems. For example, it can optimize supply chain logistics or financial modeling, enabling faster decisionmaking. The manual likely references COBIT 2019's APO02-Managed Strategy, which emphasizes leveraging technology for strategic efficiency.
Option A: To increase revenue is a secondary outcome, not the primary objective of the architecture itself.
Option C: To reduce cyberattacks is tangential; while quantum computing may impact cryptography, it's not its primary goal.
Option D: To minimize operating costs may occur indirectly, but efficiency in computation is the core focus.
Double Verification: The answer aligns with COBIT's focus on strategic technology adoption and the CGEIT domain's emphasis on efficiency through innovation. Quantum computing's primary value is computational efficiency, a key strategic consideration in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on strategic management and emerging technologies).
COBIT 2019, APO02-Managed Strategy.
ISACA Glossary (for definitions of quantum computing), available at https://www.isaca.org/resources/glossary.

Question: 616

An enterprise is planning to upgrade its current enterprise resource planning (ERP) system to remain competitive within the industry. Which of the following would be MOST helpful to facilitate a successful implementation?

A. Documenting the current ERP processes and procedures
B. Reviewing the ERP post-implementation report
C. Establishing a change and transition planning process
D. Conducting a comprehensive requirements review

Answer: D

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Strategic Management domain, emphasizes aligning IT initiatives like ERP upgrades with business objectives through thorough planning and requirements analysis. A successful

ERP implementation requires understanding business needs to ensure the system supports competitive goals.

Option D: Conducting a comprehensive requirements review is the most helpful. This involves gathering and analyzing business and functional requirements to ensure the new ERP system meets current and future needs (e.g., scalability, integration). For example, a requirements review identifies critical processes (e.g., supply chain management) and ensures the ERP aligns with industry demands. The manual likely references COBIT 2019's BAI02-Managed Requirements Definition, which prioritizes requirements analysis for successful IT projects.

Option A: Documenting the current ERP processes and procedures is useful for baseline understanding but doesn't ensure the new system meets future needs.

Option B: Reviewing the ERP post-implementation report is irrelevant, as it applies to past implementations, not the current upgrade.

Option C: Establishing a change and transition planning process is important but secondary to defining requirements, as change management follows requirements.

Double Verification: The answer aligns with COBIT's BAI02 and the CGEIT domain's focus on strategic project planning. Requirements review is a foundational step in ISACA's project management guidance.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on strategic IT project planning).

COBIT 2019, BAI02-Managed Requirements Definition.

ISACA Glossary (for definitions of ERP and requirements review), available at https://www.isaca.org/resources/glossary.

Question: 617

Which method BEST enables an enterprise to estimate the benefits of a new Software as a Service (SaaS) application?

A. Monte Carlo analysis
B. Total cost of ownership (TCO)
C. Expected monetary value
D. Heuristic methods

Answer: C

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Benefits Realization domain, focuses on evaluating IT investments to estimate and realize benefits. Estimating benefits for a SaaS application requires quantifying expected financial and operational outcomes to justify the investment.

Option C: Expected monetary value is the best method. This approach calculates the probable financial benefits (e.g., cost savings, revenue growth) by weighting potential outcomes by their probabilities. For a SaaS application, it might estimate benefits like reduced IT maintenance costs or increased productivity, factoring in uncertainties. The manual likely references COBIT 2019's APO05- Managed Portfolio, which includes value estimation techniques for IT investments.

Option A: Monte Carlo analysis is used for risk assessment, not direct benefit estimation, as it models scenarios with probabilities.

Option B: Total cost of ownership (TCO) focuses on costs, not benefits, though it complements benefit analysis.

Option D: Heuristic methods rely on subjective judgment, lacking the precision needed for benefit estimation.
Double Verification: The answer aligns with COBIT's value management processes and the CGEIT domain's emphasis on quantifying benefits. Expected monetary value is a standard financial technique in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 3: Benefits Realization (focus on benefit estimation).
COBIT 2019, APO05-Managed Portfolio.
ISACA Glossary (for definitions of expected monetary value), available at https://www.isaca.org/resources/glossary.

Question: 618

A series of cyber events impacting internet-facing business services has been successfully contained. To minimize future business risk exposure, which of the following should the board require of the IT team?

A. Review the internet service provider (ISP) contract.
B. Purchase cybersecurity insurance.
C. Conduct a business impact analysis (BIA).
D. Perform a root cause analysis.

Answer: D

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, emphasizes proactive risk management to minimize future risks after incidents. After containing cyber events, understanding their causes is critical to prevent recurrence and reduce business exposure.
Option D: Perform a root cause analysis is the best approach. This involves investigating the underlying reasons for the cyber events (e.g., vulnerabilities, misconfigurations) to identify and remediate weaknesses. For example, a root cause analysis might reveal unpatched systems, leading to improved patch management. The manual likely references COBIT 2019's APO12-Managed Risk, which includes root cause analysis as a key risk response activity.
Option A: Review the ISP contract is narrow and may not address the root causes of cyber events, which are often internal.
Option B: Purchase cybersecurity insurance mitigates financial impact but doesn't prevent future incidents.
Option C: Conduct a BIA assesses impact but doesn't identify causes, making it less immediate for risk reduction.
Double Verification: The answer aligns with COBIT's risk management processes and the CGEIT domain's focus on addressing incident causes. Root cause analysis is a standard ISACA practice postincident.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on incident response and risk mitigation).
COBIT 2019, APO12-Managed Risk.
ISACA Glossary (for definitions of root cause analysis), available at https://www.isaca.org/resources/glossary.

Question: 619

An enterprise has an overarching enterprise architecture (EA) document. The CIO is concerned that EA is not

leveraged in recent IT-enabled investments. Which of the following would BEST help to address these concerns and enforce the leveraging of EA?

A. Form a team to update EA regularly.
B. Require EA review at key milestones.
C. Publish and train on the EA document.
D. Adopt a globally recognized EA framework.

Answer: B

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, emphasizes the role of enterprise architecture (EA) in ensuring IT investments align with business strategies. If EA is not being leveraged, governance processes must enforce its use during project execution.

Option B: Require EA review at key milestones is the best approach. Integrating EA reviews into project stage gates (e.g., design, implementation) ensures that IT investments adhere to the EA's standards, principles, and roadmap. For example, a review might confirm that a new system aligns with the EA's technology stack. The manual likely references COBIT 2019's APO03-Managed Enterprise Architecture, which advocates for EA integration in project governance.

Option A: Form a team to update EA regularly is proactive but doesn't enforce EA use in projects.

Option C: Publish and train on the EA document raises awareness but lacks enforcement.

Option D: Adopt a globally recognized EA framework is unnecessary if an EA exists, as the issue is leverage, not framework choice.

Double Verification: The answer aligns with COBIT's EA governance processes and the CGEIT domain's focus on project alignment. Milestone reviews are a standard ISACA practice for EA enforcement.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on enterprise architecture).

COBIT 2019, APO03-Managed Enterprise Architecture.

ISACA Glossary (for definitions of EA), available at https://www.isaca.org/resources/glossary.

Question: 620

An enterprise wants to establish key risk indicators (KRIs) in an effort to better manage IT risk. Which of the following should be identified FIRST?

A. The enterprise risk appetite
B. Key performance metrics
C. Risk mitigation strategies
D. Enterprise architecture (EA) components

Answer: A

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, emphasizes the importance of aligning IT risk management with the enterprise's overall risk management strategy. Key risk indicators (KRIs) are metrics used to monitor potential risks and provide early warnings. To establish effective KRIs, the enterprise must first understand its risk tolerance and priorities.

Option A: The enterprise risk appetite should be identified first. Risk appetite defines the level of risk the

enterprise is willing to accept in pursuit of its objectives, guiding the selection of KRIs. For example, if the enterprise has a low risk appetite for data breaches, KRIs might focus on metrics like unauthorized access attempts. Identifying risk appetite ensures KRIs are relevant and aligned with strategic goals. The manual likely references COBIT 2019's APO12-Managed Risk, which highlights risk appetite as a foundational element of risk management.

Option B: Key performance metrics relate to performance, not risk, and are not directly relevant to KRIs.

Option C: Risk mitigation strategies are developed after identifying risks and KRIs, not before.

Option D: Enterprise architecture (EA) components may inform risk identification but are secondary to defining risk appetite.

Double Verification: The answer aligns with COBIT's APO12 and the CGEIT domain's focus on risk management foundations. Risk appetite is a prerequisite for KRI development in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on risk management and KRIs).

COBIT 2019, APO12-Managed Risk.

ISACA Glossary (for definitions of risk appetite and KRIs), available at https://www.isaca.org/resources/glossary.

Question: 621

A healthcare enterprise is procuring Internet of Things (IoT) devices to be used across its facilities. Which of the following is MOST important to establish before vendors are engaged to provide the devices?

A. Product compliance criteria
B. Patient training
C. Physical security audits
D. Vendor delivery timelines

Answer: A

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, addresses the governance of IT procurement, particularly for technologies like IoT devices in regulated industries such as healthcare. Ensuring compliance with regulatory and security standards is critical before engaging vendors.

Option A: Product compliance criteria is the most important to establish first. In healthcare, IoT devices (e.g., medical sensors) must comply with regulations like HIPAA (for data privacy) and FDA standards (for device safety). Defining compliance criteria ensures vendors provide devices that meet legal, security, and interoperability requirements, reducing risks like data breaches or patient harm. The manual likely references COBIT 2019's APO09-Managed Service Agreements, which emphasizes defining requirements before vendor engagement.

Option B: Patient training is relevant post-procurement, not before vendor engagement.

Option C: Physical security audits are important but secondary to ensuring device compliance, as audits assess deployment environments.

Option D: Vendor delivery timelines are logistical and less critical than compliance in a regulated industry.

Double Verification: The answer aligns with COBIT's APO09 and the CGEIT domain's focus on compliance-driven procurement. Compliance criteria are a priority in ISACA's governance practices for healthcare IT.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on procurement and compliance).

COBIT 2019, APO09-Managed Service Agreements.

Watermark Sample

ISACA Glossary (for definitions of compliance criteria), available at https://www.isaca.org/resources/glossary.

Question: 622

Which of the following is the MOST important characteristic of a well-defined information architecture?

A. It enables achievement of service level agreements (SLAs).
B. It addresses key stakeholder requirements.
C. It ensures compliance with regulations.
D. It supports IT strategic goals.

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, defines information architecture as the structure and organization of data and information systems to support enterprise objectives. A well-defined information architecture aligns with the enterprise's strategic IT direction.

Option D: It supports IT strategic goals is the most important characteristic. Information architecture should enable the realization of IT strategies, such as digital transformation or data-driven decisionmaking, by ensuring data is organized, accessible, and secure. For example, a robust architecture supports goals like real-time analytics by integrating disparate data sources. The manual likely references COBIT 2019's APO03-Managed Enterprise Architecture, which emphasizes aligning architecture with strategic objectives.

Option A: It enables achievement of SLAs is a benefit but not the primary characteristic, as SLAs are operational.

Option B: It addresses key stakeholder requirements is important but secondary to strategic alignment, as stakeholder needs are a subset of broader goals.

Option C: It ensures compliance with regulations is critical but not the defining characteristic, as compliance is one of many strategic goals.

Double Verification: The answer aligns with COBIT's APO03 and the CGEIT domain's focus on strategic alignment. Supporting IT strategic goals is the core purpose of information architecture in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on information architecture).

COBIT 2019, APO03-Managed Enterprise Architecture.

ISACA Glossary (for definitions of information architecture), available at https://www.isaca.org/resources/glossary.

Question: 623

Which of the following is MOST important to consider when monitoring the performance of IT resources?

A. Business impact analysis (BIA)
B. End-user feedback
C. Centralized log analysis
D. Service level requirements

Answer: D

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, emphasizes monitoring IT resource performance to ensure alignment with business expectations. Performance monitoring requires clear, measurable criteria tied to service delivery.
Option D: Service level requirements is the most important to consider. These requirements, often defined in service level agreements (SLAs), specify performance metrics (e.g., uptime, response time) that IT resources must meet to support business operations. Monitoring against these requirements ensures IT delivers expected value. For example, if an SLA requires 99.9% system availability, performance monitoring focuses on this metric. The manual likely references COBIT 2019's APO09-Managed Service Agreements, which prioritizes service level monitoring.
Option A: Business impact analysis (BIA) assesses disruption impacts, not ongoing performance. Option B: End-user feedback is valuable but subjective and less precise than service level metrics. Option C: Centralized log analysis supports security and troubleshooting, not direct performance monitoring.
Double Verification: The answer aligns with COBIT's APO09 and the CGEIT domain's focus on service management. Service level requirements are the primary benchmark for IT performance in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on service performance monitoring).
COBIT 2019, APO09-Managed Service Agreements.
ISACA Glossary (for definitions of service level requirements), available at https://www.isaca.org/resources/glossary.

Question: 624

Forensic analysis revealed an attempted breach of a personnel database containing sensitive data. A subsequent investigation found that no one within the enterprise was aware of the breach attempt, even though logs recorded the unauthorized access actions. To prevent a similar situation in the future, what is MOST important for IT governance to require?

A. Periodic analyses of logs and databases for unusual activity
B. A review of the information security and risk management frameworks
C. The creation of a comprehensive data management and storage policy
D. The implementation of an intrusion detection and reporting process

Answer: D

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, addresses the need for proactive detection and response to security incidents to minimize risks. The undetected breach attempt highlights a gap in real-time monitoring and alerting.
Option D: The implementation of an intrusion detection and reporting process is the most important. An intrusion detection system (IDS) monitors network and system activities for unauthorized access, generating alerts for immediate response. This would have ensured the breach attempt was detected and reported in real-time, preventing potential data loss. The manual likely references COBIT 2019's DSS05-Managed Security Services, which emphasizes intrusion detection as a critical security control.
Option A: Periodic analyses of logs and databases is reactive and may not detect breaches in time, unlike real-time IDS.
Option B: A review of security and risk frameworks is broad and long-term, not addressing the immediate

detection gap.

Option C: A comprehensive data management policy focuses on data governance, not real-time breach detection.

Double Verification: The answer aligns with COBIT's DSS05 and the CGEIT domain's focus on security incident detection. Intrusion detection is a standard ISACA recommendation for preventing undetected breaches.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on security incident detection).
COBIT 2019, DSS05-Managed Security Services.
ISACA Glossary (for definitions of intrusion detection), available at https://www.isaca.org/resources/glossary.

Question: 625

Which of the following BEST enables informed IT investment decisions?

A. Business case
B. Technology roadmap
C. Program plan
D. Risk classification

Answer: A

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Benefits Realization domain, emphasizes the importance of structured decision-making for IT investments to ensure they deliver value. A business case provides a comprehensive justification for an investment, including objectives, costs, benefits, risks, and alignment with business goals. It enables stakeholders to make informed decisions by presenting a clear rationale and expected outcomes. For example, a business case for a new CRM system would detail projected revenue increases and implementation costs. The manual likely references COBIT 2019's APO05-Managed Portfolio, which highlights the business case as a critical tool for investment evaluation.

Option B: Technology roadmap outlines future technology plans but lacks the detailed financial and benefit analysis needed for investment decisions.

Option C: Program plan focuses on execution details, not the justification for investment.

Option D: Risk classification addresses risk but doesn't encompass the full scope of benefits and costs.

Double Verification: The answer aligns with COBIT's APO05 and the CGEIT domain's focus on value- driven investment decisions. The business case is a standard ISACA tool for informed decisionmaking.

ISACA CGEIT Review Manual 8th Edition, Domain 3: Benefits Realization (focus on investment decision-making).
COBIT 2019, APO05-Managed Portfolio.
ISACA Glossary (for definitions of business case), available at https://www.isaca.org/resources/glossary.

Question: 626

What is the BEST way for a board of directors to improve its ability to identify material changes to the enterprise IT risk profile?

A. Require management to present a comprehensive list of risks.
B. Require the implementation of a security incident and event management (SIEM) tool.
C. Review the key risk indicators (KRIs) on a regular basis.
D. Focus on key performance indicators (KPIs) that predict future business performance.

Answer: C

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, stresses the importance of proactive risk monitoring to ensure the board is aware of material changes to the IT risk profile. Key risk indicators (KRIs) are metrics that provide early warnings of potential risks, such as increased cyber threats or system failures. Regular KRI reviews enable the board to detect shifts in the risk profile (e.g., a spike in unauthorized access attempts) and take timely action. The manual likely references COBIT 2019's APO12-Managed Risk, which emphasizes KRIs for risk oversight.

Option A: Comprehensive list of risks is static and less effective for ongoing monitoring.

Option B: SIEM tool is operational and supports detection but doesn't directly provide board-level risk insights.

Option D: KPIs focus on performance, not risk, and are less relevant for risk profile changes. Double Verification: The answer aligns with COBIT's APO12 and the CGEIT domain's focus on risk monitoring. KRIs are a standard ISACA tool for board-level risk oversight.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on risk monitoring). COBIT 2019, APO12-Managed Risk.

ISACA Glossary (for definitions of KRIs), available at https://www.isaca.org/resources/glossary.

Question: 627

A newly established IT steering committee is concerned whether a system is meeting availability objectives. Which of the following will provide the BEST information to make an assessment?

A. Critical success factors (CSFs)
B. Performance indicators
C. Capability maturity levels
D. Balanced scorecard

Answer: B

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, emphasizes monitoring system performance against defined objectives, such as availability. Performance indicators, often tied to service level agreements (SLAs), provide specific, measurable data (e.g., system uptime percentage) to assess whether availability objectives are met. For example, a performance indicator showing 99.8% uptime directly informs the committee. The manual likely references COBIT 2019's APO09-Managed Service Agreements, which prioritizes performance indicators for service monitoring.

Option A: Critical success factors (CSFs) define conditions for success but are less specific than performance metrics.

Option C: Capability maturity levels assess process maturity, not system availability.

Option D: Balanced scorecard provides a broad performance overview but is less focused on specific availability metrics.

Double Verification: The answer aligns with COBIT's APO09 and the CGEIT domain's focus on service performance. Performance indicators are the primary ISACA tool for availability assessment.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on service monitoring).
COBIT 2019, APO09-Managed Service Agreements.
ISACA Glossary (for definitions of performance indicators), available at https://www.isaca.org/resources/glossary.

Question: 628

An enterprise recently acquired technology that will enable it to offer products to customers through a mobile device application. The business is eager to use this technology as soon as possible for products currently offered through legacy IT systems. What is the CIO's MAIN responsibility?

A. Ensure proper metrics are established to measure technology usage throughout the enterprise.
B. Ensure business units are aware of new opportunities available with the acquired technology.
C. Ensure the enterprise architecture (EA) is reviewed and updated.
D. Ensure risk associated with implementation and support of the new technology is properly managed.

Answer: D

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, underscores the CIO's role in managing risks associated with new technology deployments. Rapid adoption of a mobile application introduces risks (e.g., security vulnerabilities, integration issues), which the CIO must prioritize to protect the enterprise. Ensuring risk is properly managed involves risk assessments, mitigation plans, and compliance checks (e.g., for data privacy). The manual likely references COBIT 2019's APO12-Managed Risk, which emphasizes risk management for new IT initiatives.
Option A: Metrics for usage are important but secondary to risk management during implementation. Option B: Business unit awareness is a communication task, not the CIO's main responsibility. Option C: EA review is relevant but less urgent than addressing immediate implementation risks. Double Verification: The answer aligns with COBIT's APO12 and the CGEIT domain's focus on risk management for new technologies. Risk management is a core CIO responsibility in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on technology implementation risks).
COBIT 2019, APO12-Managed Risk.
ISACA Glossary (for definitions of risk management), available at https://www.isaca.org/resources/glossary.

Question: 629

Which of the following is the BEST way for a CIO to provide senior business management with increased visibility to the overall performance of the IT operation?

A. Develop key risk indicators (KRIs).
B. Provide return on investment (ROI) reports.
C. Develop key performance indicators (KPIs).
D. Provide service level agreement (SLA) performance statistics.

Answer: C

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, highlights the need for IT performance reporting to ensure transparency with senior management. Key performance indicators (KPIs) provide a comprehensive view of IT operations, covering metrics like system availability, project delivery, and cost efficiency. KPIs align IT performance with business objectives, offering a holistic perspective. The manual likely references COBIT 2019's MEA01-Monitor, Evaluate, and Assess Performance, which emphasizes KPIs for performance visibility.
Option A: KRIs focus on risks, not overall performance.
Option B: ROI reports are financial and project-specific, not comprehensive.
Option D: SLA performance statistics are narrow, focusing only on service delivery.
Double Verification: The answer aligns with COBIT's MEA01 and the CGEIT domain's focus on performance reporting. KPIs are the standard ISACA tool for IT performance visibility.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on performance reporting).
COBIT 2019, MEA01-Monitor, Evaluate, and Assess Performance.
ISACA Glossary (for definitions of KPIs), available at https://www.isaca.org/resources/glossary.

Question: 630

Which of the following is the PRIMARY outcome of using a comprehensive architecture framework?
A. Key third-party relationships are supported.
B. Business goal conflicts are identified.
C. Relevant controls are identified.
D. Organizational management policies are developed.

Answer: B

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Strategic Management domain, describes a comprehensive architecture framework (e.g., enterprise architecture) as a tool to align IT with business strategies. The primary outcome is identifying business goal conflicts, as the framework maps business processes, systems, and strategies, revealing misalignments (e.g., conflicting departmental objectives). This enables resolution to ensure cohesive strategy execution. The manual likely references COBIT 2019's APO03-Managed Enterprise Architecture, which highlights conflict
identification as a key benefit.
Option A: Third-party relationships are secondary and not the primary focus.
Option C: Relevant controls are an outcome but not the primary one, as controls follow alignment.
Option D: Management policies are unrelated to architecture frameworks.
Double Verification: The answer aligns with COBIT's APO03 and the CGEIT domain's focus on strategic alignment. Conflict identification is a core outcome of EA in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on enterprise architecture).
COBIT 2019, APO03-Managed Enterprise Architecture.
ISACA Glossary (for definitions of architecture framework), available at https://www.isaca.org/resources/glossary.

Question: 631

In which of the following situations is it acceptable to retain data beyond the stated policy?

A. The business created an analytics model based on historical records.
B. There is a high probability that the enterprise will enter into litigation.
C. New data privacy regulations are expected in a few months.
D. A core system database is going through an upgrade.

Answer: B

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, addresses data retention policies and exceptions, particularly in regulated environments. Retaining data beyond policy is acceptable when legally justified, such as a high probability of litigation, where data may be required as evidence. This ensures compliance with legal obligations and avoids penalties. The manual likely references COBIT 2019's BAI09-Managed Assets, which includes data retention for legal purposes.

Option A: Analytics model does not justify violating policy, as analytics can use anonymized data. Option C: Expected regulations are speculative and not a valid exception.

Option D: Database upgrade is technical and unrelated to retention policy exceptions.

Double Verification: The answer aligns with COBIT's BAI09 and the CGEIT domain's focus on compliance. Litigation is a standard ISACA exception for data retention.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on data governance).

COBIT 2019, BAI09-Managed Assets.

ISACA Glossary (for definitions of data retention), available at https://www.isaca.org/resources/glossary.

Question: 632

A CIO realizes a significant change is required in the way IT responds to key external customers and needs to gain support from the enterprise to address this situation. What should be done FIRST?

A. Empower key IT staff to implement a solution.
B. Establish new customer service policies.
C. Engage customer service training providers.
D. Engage the IT steering committee.

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, emphasizes the role of the IT steering committee in aligning IT initiatives with business needs. To gain enterprise support for a significant change in customer response, the CIO should first engage the IT steering committee to secure strategic alignment, resources, and stakeholder buy-in. This ensures the change is prioritized and supported across the enterprise. The manual likely references COBIT 2019's EDM01-Ensured Governance Framework Setting and Maintenance, which highlights the steering committee's role in strategic decisions.

Option A: Empower IT staff is premature without strategic approval.

Option B: New policies require prior stakeholder agreement.

Option C: Training providers are a tactical step, not the first action.

Double Verification: The answer aligns with COBIT's EDM01 and the CGEIT domain's focus on governance structures. The steering committee is the primary ISACA mechanism for strategic change.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on steering committee roles).
COBIT 2019, EDM01-Ensured Governance Framework Setting and Maintenance.
ISACA Glossary (for definitions of IT steering committee), available at https://www.isaca.org/resources/glossary.

Question: 633

Which of the following provides the STRONGEST indication that IT governance is well established within an organizational culture?

A. Benefits of IT governance are realized throughout the organization.
B. There is awareness of IT metrics throughout the organization.
C. IT governance defines how IT projects should be assessed.
D. IT performance metrics are defined in the balanced scorecard.

Answer: B

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, describes well- established IT governance as a culture where IT aligns with business objectives and is embedded in organizational processes. Awareness of IT metrics throughout the organization indicates that governance is ingrained, as employees at all levels understand and use metrics (e.g., KPIs, KRIs) to guide decisions. This reflects a mature governance culture. The manual likely references COBIT 2019's EDM01-Ensured Governance Framework Setting and Maintenance, which emphasizes cultural integration of governance.
Option A: Benefits realized is an outcome, not an indication of cultural establishment.
Option C: Project assessment definitions are procedural, not cultural.
Option D: Balanced scorecard metrics are specific and not as broad as organization-wide metric awareness.
Double Verification: The answer aligns with COBIT's EDM01 and the CGEIT domain's focus on governance culture. Metric awareness is a key ISACA indicator of governance maturity.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on governance culture).
COBIT 2019, EDM01-Ensured Governance Framework Setting and Maintenance.
ISACA Glossary (for definitions of IT governance), available at https://www.isaca.org/resources/glossary.

Question: 634

When developing IT risk management policies and standards, it is MOST important to align them with:

A. Best practices for IT risk management.
B. The corporate risk culture.
C. Enterprise goals and objectives.
D. The enterprise risk management (ERM) framework.

Answer: C

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, emphasizes that IT risk management policies and standards must support the enterprise's strategic objectives to ensure alignment with business priorities. Enterprise goals and objectives provide the foundation for IT risk management, ensuring that policies address risks that could hinder strategic outcomes (e.g., market expansion, regulatory compliance). For example, if an enterprise goal is to enhance customer trust, risk policies might prioritize cybersecurity. The manual likely references COBIT 2019's APO12- Managed Risk, which stresses aligning risk management with business objectives.

Option A: Best practices are important but generic and may not reflect specific enterprise needs. Option B: Corporate risk culture influences risk management but is secondary to strategic goals. Option D: ERM framework is a broader structure that IT risk management should integrate with, but enterprise goals are the primary driver.

Double Verification: The answer aligns with COBIT's APO12 and the CGEIT domain's focus on business alignment. Enterprise goals are the primary focus for risk policy alignment in ISACA's frameworks.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on risk policy alignment).
COBIT 2019, APO12-Managed Risk.
ISACA Glossary (for definitions of risk management), available at https://www.isaca.org/resources/glossary.

Question: 635

Senior management is concerned about the unauthorized use of third-party data that is stored within the enterprise's data repositories. Which of the following is the BEST way to address this concern?

A. Communicate consequences for staff who misuse third-party data.
B. Ensure all third-party data in transit is encrypted.
C. Establish data ownership with clear accountabilities.
D. Establish optimal retention periods for third-party data.

Answer: C

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, addresses data governance to ensure proper management and protection of data, including third-party data. Establishing data ownership with clear accountabilities ensures that specific individuals or roles are responsible for overseeing third-party data, preventing unauthorized use through defined policies and controls. For example, a data owner can enforce access restrictions and monitor usage. The manual likely references COBIT 2019's APO14-Managed Data, which emphasizes data ownership for governance.

Option A: Communicate consequences is reactive and less effective than proactive ownership. Option B: Encrypt data in transit addresses security but not unauthorized internal use. Option D: Retention periods manage data lifecycle but don't directly prevent misuse.

Double Verification: The answer aligns with COBIT's APO14 and the CGEIT domain's focus on data governance. Data ownership is a core ISACA principle for data protection.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on data governance).
COBIT 2019, APO14-Managed Data.
ISACA Glossary (for definitions of data ownership), available at https://www.isaca.org/resources/glossary.

Question: 636

Which of the following roles is accountable for the confidentiality, integrity, and availability of information within an enterprise?

A. Data owner
B. Lead legal counsel
C. Risk manager
D. Data custodian

Answer: A

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, defines roles and responsibilities for information security. The data owner is accountable for ensuring the confidentiality, integrity, and availability (CIA) of information, as they have authority over specific data sets and define security requirements. For example, a data owner for customer data ensures access controls and data protection measures are in place. The manual likely references COBIT 2019's APO14-Managed Data, which assigns CIA accountability to data owners.

Option B: Lead legal counsel advises on legal compliance, not CIA.

Option C: Risk manager oversees risk but not specific data accountability.

Option D: Data custodian implements controls but is not accountable for CIA.

Double Verification: The answer aligns with COBIT's APO14 and the CGEIT domain's focus on data roles. Data owner accountability is a standard ISACA principle.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on data roles).

COBIT 2019, APO14-Managed Data.

ISACA Glossary (for definitions of data owner), available at https://www.isaca.org/resources/glossary.

Question: 637

What is the BEST way to demonstrate alignment of IT projects with long-term business objectives?

A. Service level agreements (SLAs)
B. Portfolio management
C. Enterprise architecture (EA)
D. Business impact analysis (BIA)

Answer: C

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Strategic Management domain, emphasizes aligning IT projects with business objectives through structured frameworks. Enterprise architecture (EA) provides a blueprint that maps IT projects to long-term business strategies, ensuring alignment with goals like digital transformation or market expansion. For example, EA ensures a new IT system supports strategic objectives by defining standards and roadmaps. The manual likely references COBIT 2019's APO03-Managed Enterprise Architecture, which focuses on strategic alignment. Option A: SLAs focus on operational performance, not strategic alignment.

Option B: Portfolio management prioritizes projects but doesn't inherently demonstrate alignment. Option D: BIA assesses impacts, not strategic alignment.

Double Verification: The answer aligns with COBIT's APO03 and the CGEIT domain's focus on strategic alignment. EA is the primary ISACA tool for demonstrating alignment.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on enterprise architecture).
COBIT 2019, APO03-Managed Enterprise Architecture.
ISACA Glossary (for definitions of EA), available at https://www.isaca.org/resources/glossary.

Question: 638

Which of the following would BEST enable an enterprise to ensure selected cloud vendors meet stringent regulatory requirements?

A. Stage gate reviews
B. Risk assessment
C. Internal audit report
D. Third-party audit reports

Answer: D

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, addresses vendor management in regulated environments. Third-party audit reports provide independent verification that cloud vendors comply with stringent regulatory requirements (e.g., GDPR, HIPAA), offering evidence of controls and certifications (e.g., SOC 2, ISO 27001). These reports are critical for due diligence. The manual likely references COBIT 2019's APO10-Managed Vendors, which emphasizes third-party assurance for compliance.
Option A: Stage gate reviews are project management checkpoints, not vendor compliance tools. Option B: Risk assessment evaluates risks but lacks independent verification.
Option C: Internal audit report assesses internal controls, not vendor compliance.
Double Verification: The answer aligns with COBIT's APO10 and the CGEIT domain's focus on vendor governance. Third-party audits are a standard ISACA requirement for vendor compliance.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on vendor management).
COBIT 2019, APO10-Managed Vendors.
ISACA Glossary (for definitions of third-party audit), available at https://www.isaca.org/resources/glossary.

Question: 639

Which of the following will BEST help to ensure enterprise IT risk is effectively managed?

A. Establishing an audit committee that reports to the board
B. Establishing roles and responsibilities for IT risk at the senior management level
C. Identifying the lowest IT risks and outsourcing the related IT functions
D. Assigning a project sponsor and project manager to implement an IT risk register

Answer: B

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, stresses the importance of clear roles

and responsibilities for effective IT risk management. Establishing roles and responsibilities at the senior management level ensures accountability, strategic oversight, and integration of risk management into decision-making. For example, a chief risk officer might oversee IT risk policies. The manual likely references COBIT 2019's EDM03-Ensured Risk Optimization, which emphasizes senior-level accountability.
Option A: Audit committee oversees compliance, not direct risk management.
Option C: Outsourcing low risks is tactical and doesn't address overall risk management.
Option D: Project sponsor and manager are project-specific, not enterprise-wide.
Double Verification: The answer aligns with COBIT's EDM03 and the CGEIT domain's focus on risk governance. Senior-level roles are critical in ISACA's risk management framework.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on risk governance).
COBIT 2019, EDM03-Ensured Risk Optimization.
ISACA Glossary (for definitions of risk management roles), available at https://www.isaca.org/resources/glossary.

Question: 640

An enterprise has well-designed procurement and vendor risk management policies that are intended to prevent biased decision-making. However, a pattern of ethical violations indicates that vendor selection may have been inappropriately influenced by non-work-related incentives provided to decision makers. Which of the following should be done FIRST in response to this issue?

A. Revise the procurement and vendor risk management policies.
B. Conduct a root cause analysis and remediate based on findings.
C. Document the critical success factors (CSFs) for the procurement policies.
D. Establish and communicate strict penalties for biased vendor selection.

Answer: B

Explanation:

Comprehensive and Detailed
The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, addresses ethical governance and policy enforcement. When ethical violations occur, the first step is to conduct a root cause analysis to identify why policies failed (e.g., lack of oversight, inadequate controls) and remediate based on findings. This ensures targeted solutions, such as enhanced monitoring or training. The manual likely references COBIT 2019's MEA03-Managed Compliance with External Requirements, which includes root cause analysis for governance issues.
Option A: Revise policies is premature without understanding the cause.
Option C: Document CSFs is unrelated to addressing violations.
Option D: Strict penalties may deter but don't address underlying issues.
Double Verification: The answer aligns with COBIT's MEA03 and the CGEIT domain's focus on ethical governance. Root cause analysis is a standard ISACA response to policy failures.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on ethical governance).
COBIT 2019, MEA03-Managed Compliance with External Requirements.
ISACA Glossary (for definitions of root cause analysis), available at https://www.isaca.org/resources/glossary.

Question: 641

To define the risk management strategy, which of the following MUST be set by the board of directors?

A. Risk management process
B. Risk identification plan
C. Risk treatment plan
D. Risk appetite

Answer: D

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Risk Optimization domain, states that the board of directors is responsible for setting the risk appetite, which defines the level of risk the enterprise is willing to accept to achieve its objectives. This guides the risk management strategy, ensuring alignment with business goals. For example, a conservative risk appetite might prioritize cybersecurity investments. The manual likely references COBIT 2019's EDM03-Ensured Risk Optimization, which assigns risk appetite to the board.

Option A: Risk management process is operational and defined by management.

Option B: Risk identification plan is tactical and not a board responsibility.

Option C: Risk treatment plan follows risk appetite setting.

Double Verification: The answer aligns with COBIT's EDM03 and the CGEIT domain's focus on board responsibilities. Risk appetite is a core ISACA board duty.

ISACA CGEIT Review Manual 8th Edition, Domain 4: Risk Optimization (focus on board roles). COBIT 2019, EDM03-Ensured Risk Optimization.

ISACA Glossary (for definitions of risk appetite), available at https://www.isaca.org/resources/glossary.

Question: 642

Which of the following is MOST important for the successful establishment of an ethics program?

A. Defined whistleblower processes
B. Culture of accountability and responsibility
C. Defined roles and responsibilities
D. Clear mission and vision statements

Answer: B

Explanation:

Comprehensive and Detailed

The CGEIT Review Manual 8th Edition, in its Governance of Enterprise IT domain, emphasizes that an ethics program requires a culture of accountability and responsibility to succeed. This culture ensures that ethical behavior is embedded in organizational values, encouraging employees to act with integrity. For example, leadership modeling ethical behavior fosters trust and compliance. The manual likely references COBIT 2019's EDM01-Ensured Governance Framework Setting and Maintenance, which highlights cultural factors in governance.

Option A: Whistleblower processes are important but secondary to culture.

Option C: Roles and responsibilities support the program but are not the most critical.

Option D: Mission and vision statements are foundational but less directly tied to ethics.

Double Verification: The answer aligns with COBIT's EDM01 and the CGEIT domain's focus on ethical governance. Culture is a key ISACA factor for ethics programs.

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT (focus on ethics programs).
COBIT 2019, EDM01-Ensured Governance Framework Setting and Maintenance.
ISACA Glossary (for definitions of ethics program), available at https://www.isaca.org/resources/glossary.

Question: 643

An enterprise's IT department has failed to deliver required solutions on time due to insufficient resource allocation, resulting in a longer time to market. Which of the following is the BEST way for the chief information officer (CIO) to address this situation?

A. Implement a new IT change management procedure.
B. Evaluate the availability and capacity planning process.
C. Benchmark IT staffing levels against similar organizations in the industry.
D. Direct the project management office (PMO) to review and prioritize IT projects.

Answer: B

Explanation:

The issue described in the question is the failure to deliver IT solutions on time due to insufficient resource allocation, which points to a problem in resource management, specifically in capacity and availability planning. According to the CGEIT Review Manual 8th Edition, effective IT resource management involves ensuring that IT resources (human, technological, and financial) are allocated efficiently to meet enterprise objectives. The manual emphasizes the importance of capacity planning to align resource availability with project demands, which directly addresses delays caused by resource shortages.
Extract from CGEIT Review Manual 8th Edition (Domain 2: IT Resources):"Capacity planning ensures that IT resources are sufficient to meet current and future business requirements in a cost-effective manner. It involves assessing the availability of resources, forecasting demand, and aligning resource allocation with strategic priorities to avoid bottlenecks and delays in delivery." (Approximate reference: Domain 2, Section on Resource Management)
Evaluating the availability and capacity planning process (option B) is the most direct approach to identifying and resolving resource allocation issues. This process involves reviewing current resource utilization, forecasting future needs, and ensuring that resources are allocated to high-priority projects to reduce time-to-market delays.
Why not the other options?
A . Implement a new IT change management procedure: Change management procedures focus on controlling changes to IT systems and services, not on addressing resource allocation or capacity issues. This option is unrelated to the root cause of the problem.
C . Benchmark IT staffing levels against similar organizations: While benchmarking can provide insights into staffing adequacy, it is a secondary step that does not directly address the immediate issue of resource allocation and capacity planning. It may be useful later but is not the first step. D . Direct the PMO to review and prioritize IT projects: While project prioritization is important, it does not address the underlying issue of insufficient resource allocation. Prioritization may help focus efforts, but without adequate resources, delays will persist.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 2: IT Resources, Section on Resource Management and Capacity Planning.
ISACA CGEIT Study Guide, Chapter on IT Resource Optimization.

Question: 644

A publicly traded enterprise wants to demonstrate that its board of directors is providing adequate strategic oversight of IT. Which of the following BEST supports this objective?

A. Annual IT governance communication to all staff.
B. Press releases targeted at large investors.
C. Inclusion of IT governance reporting in the annual report.
D. Annual presentation of IT performance metrics.

Answer: C

Explanation:

Demonstrating adequate strategic oversight of IT by the board involves providing transparent, formal, and authoritative evidence to stakeholders, particularly for a publicly traded enterprise. The CGEIT Review Manual 8th Edition highlights that IT governance reporting in official documents, such as the annual report, is a key mechanism to communicate the board's oversight role to shareholders, regulators, and other stakeholders.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"The board of directors is responsible for ensuring that IT governance is aligned with enterprise objectives and that oversight is transparent to stakeholders. Including IT governance reporting in the annual report provides a formal mechanism to demonstrate accountability, strategic alignment, and oversight to shareholders and regulatory bodies." (Approximate reference: Domain 1, Section on Governance Framework and Reporting)

Including IT governance reporting in the annual report (option C) directly addresses the need to demonstrate board oversight in a formal, public, and credible manner, as it reaches shareholders and regulators who expect such disclosures in official financial and governance documents.

Why not the other options?

A . Annual IT governance communication to all staff: Internal communication to staff is important for alignment but does not directly demonstrate board oversight to external stakeholders like investors or regulators.

B . Press releases targeted at large investors: Press releases are informal and may lack the credibility and permanence of an annual report. They are not a standard mechanism for governance reporting. D . Annual presentation of IT performance metrics: While performance metrics are useful, a presentation is typically internal or limited in scope and does not provide the formal, public disclosure required to demonstrate board oversight.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Governance Reporting and Stakeholder Communication.

ISACA CGEIT Study Guide, Chapter on Governance Frameworks.

Question: 645

An enterprise has established a goal of leveraging AI as a source of strategic advantage. Which of the following should be done FIRST when developing the related IT strategy?

A. Document requirements mapped to each business function.
B. Benchmark how other IT organizations are leveraging AI.
C. Define the IT infrastructure requirements for AI implementation.
D. Define an operational level agreement (OLA) between IT and business functions.

Answer: A

Explanation:

Developing an IT strategy to leverage AI requires a clear understanding of business needs and objectives to ensure alignment. The CGEIT Review Manual 8th Edition emphasizes that the first step in strategic IT planning is to identify and document business requirements, as these drive the development of an IT strategy that supports enterprise goals.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"The development of an IT strategy begins with a thorough understanding of business requirements and objectives. Documenting requirements mapped to business functions ensures that the IT strategy is aligned with enterprise goals and delivers value." (Approximate reference: Domain 4, Section on Strategic Alignment)

Documenting requirements mapped to each business function (option A) ensures that the AI strategy is tailored to specific business needs, such as improving customer experience, optimizing operations, or enhancing decision-making. This step precedes technical or operational considerations, as it establishes the foundation for the strategy.

Why not the other options?

B . Benchmark how other IT organizations are leveraging AI: Benchmarking is useful for gaining insights but is a secondary step that should follow the identification of business requirements. Without clear requirements, benchmarking may lead to irrelevant comparisons.

C . Define the IT infrastructure requirements for AI implementation: Infrastructure requirements are technical details that come after understanding business needs and defining the scope of AI use cases.

D . Define an operational level agreement (OLA) between IT and business functions: OLAs are operational agreements that support implementation, not strategy development. They are premature at this stage.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Strategic IT Planning.

ISACA CGEIT Study Guide, Chapter on IT Strategy Development.

Question: 646

Which of the following should be the FIRST step to ensure IT resources have the appropriate skills and experience level to support enterprise objectives?

A. Determining the required competencies.
B. Providing training to IT personnel.
C. Developing an IT skills matrix.
D. Monitoring resource performance.

Answer: A

Explanation:

Ensuring that IT resources have the appropriate skills and experience begins with identifying the competencies required to meet enterprise objectives. The CGEIT Review Manual 8th Edition stresses that competency assessment is the foundational step in IT resource management to align human capital with strategic goals.

Extract from CGEIT Review Manual 8th Edition (Domain 2: IT Resources):"Determining the required competencies for IT roles is the first step in ensuring that human resources are capable of supporting enterprise objectives. This involves identifying the skills, knowledge, and experience needed to deliver IT services and projects effectively." (Approximate reference: Domain 2, Section on Human Resource Management)

Determining the required competencies (option A) establishes a baseline for assessing current capabilities, identifying gaps, and planning interventions like training or recruitment. This step must precede actions like developing a skills matrix or providing training, as those depend on knowing what competencies

are needed.

Why not the other options?

B . Providing training to IT personnel: Training is a follow-up action after identifying competency gaps, which requires knowing the required competencies first.

C . Developing an IT skills matrix: A skills matrix is a tool to document and track competencies, but it cannot be created without first defining what competencies are required.

D . Monitoring resource performance: Performance monitoring is ongoing but does not address the initial need to define required skills and experience.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 2: IT Resources, Section on Competency Management.

ISACA CGEIT Study Guide, Chapter on IT Resource Planning.

Question: 647

New legislation requires an enterprise to report cybersecurity incidents to a government agency within a defined timeline. Which of the following should be the FIRST course of action?

A. Establish an incident reporting system and hotline.

B. Require automation of incident reporting to agencies.

C. Establish a cybersecurity incident manager role.

D. Understand requirements and definitions for reportable incidents.

Answer: D

Explanation:

New legislation introduces compliance requirements that must be clearly understood before taking action. The CGEIT Review Manual 8th Edition emphasizes that the first step in addressing regulatory changes is to thoroughly understand the requirements, including definitions, scope, and timelines, to ensure compliance and avoid penalties.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"When new regulations are introduced, the first step is to understand the specific requirements, including what constitutes a reportable incident, the timeline for reporting, and the format required. This ensures that subsequent actions are aligned with regulatory expectations." (Approximate reference: Domain 3, Section on Regulatory Compliance)

Understanding the requirements and definitions for reportable incidents (option D) is critical to ensure that the enterprise knows what incidents must be reported, within what timeframe, and in what manner. This step informs the design of systems, roles, or processes to meet the legislation's demands.

Why not the other options?

A . Establish an incident reporting system and hotline: A reporting system is a subsequent step that depends on understanding what incidents need to be reported.

B . Require automation of incident reporting to agencies: Automation is premature without knowing the specific reporting requirements and formats.

C . Establish a cybersecurity incident manager role: While a dedicated role may be needed, it is not the first step, as the role's responsibilities depend on the regulatory requirements.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Compliance and Regulatory Risk.

ISACA CGEIT Study Guide, Chapter on Risk Management and Compliance.

Question: 648

Upcoming IT-related regulations carry costly penalties for an enterprise. The issuing regulatory agency has a

history of weak enforcement. The IT steering committee should FIRST direct management to:

A. Develop mitigation plans for noncompliance.
B. Update the enterprise architecture (EA).
C. Evaluate the impact of the emerging risk.
D. Perform benchmarking activities.

Answer: C

Explanation:

When faced with new regulations, the first step is to assess the risk they pose to the enterprise, including the likelihood and impact of noncompliance, even if enforcement is historically weak. The CGEIT Review Manual 8th Edition underscores that risk evaluation is the initial step in addressing emerging risks to prioritize actions and allocate resources effectively.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"Evaluating the impact of emerging risks, such as new regulations, is the first step in the risk management process. This involves assessing the potential consequences of noncompliance, including financial, operational, and reputational impacts, as well as the likelihood of enforcement." (Approximate reference: Domain 3, Section on Risk Assessment)

Evaluating the impact of the emerging risk (option C) allows the enterprise to understand the potential penalties, operational disruptions, and reputational damage, as well as the likelihood of enforcement given the agency's history. This assessment informs whether mitigation plans, architecture updates, or other actions are necessary.

Why not the other options?

A . Develop mitigation plans for noncompliance: Mitigation plans are developed after assessing the risk's impact and likelihood, as the assessment determines the scope and urgency of mitigation.

B . Update the enterprise architecture (EA): Updating the EA may be a subsequent action if the risk assessment identifies specific architectural gaps, but it is not the first step.

D . Perform benchmarking activities: Benchmarking is not directly relevant to assessing regulatory risk and is a secondary activity at best.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Risk Assessment and Management.

ISACA CGEIT Study Guide, Chapter on Risk Evaluation.

Question: 649

Which of the following is the MOST important success factor when adopting an enterprise IT governance framework?

A. Implementing an enterprise risk management (ERM) framework.
B. Aligning to the enterprise-specific business environment.
C. Complying with legal and regulatory requirements.
D. Using a globally accepted IT governance framework.

Answer: B

Explanation:

The success of an IT governance framework depends on its alignment with the enterprise's unique business environment, including its goals, culture, and operational context. The CGEIT Review Manual 8th Edition emphasizes that governance frameworks must be tailored to the enterprise's specific needs to ensure relevance and effectiveness.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"The most critical factor for successful IT governance is aligning the framework with the enterprise's business environment, including its strategic objectives, organizational structure, and operational needs. A one-size-fits-all approach is less effective than a tailored framework that reflects the enterprise's unique context." (Approximate reference: Domain 1, Section on Governance Framework Design) Aligning to the enterprise-specific business environment (option B) ensures that the governance framework supports business objectives, integrates with existing processes, and is accepted by stakeholders, making it the most important success factor.

Why not the other options?

A . Implementing an enterprise risk management (ERM) framework: While ERM is important, it is a component of governance, not the primary success factor for adopting the framework itself.

C . Complying with legal and regulatory requirements: Compliance is a requirement but not the most critical factor for overall success, as governance extends beyond compliance to value delivery and strategic alignment.

D . Using a globally accepted IT governance framework: Globally accepted frameworks (e.g., COBIT) provide a starting point, but without customization to the enterprise's context, they may not be effective.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Framework Adoption and Customization.

ISACA CGEIT Study Guide, Chapter on IT Governance Frameworks.

Question: 650

An IT governance committee is defining a risk management policy for a portfolio of IT-enabled investments. Which of the following should be the PRIMARY consideration when developing the policy?

A. Risk appetite of the enterprise.
B. Possible investment failures.
C. Risk management framework.
D. Value obtained with minimum risk.

Answer: A

Explanation:

The risk management policy for IT-enabled investments must reflect the enterprise's risk appetite, which defines the level of risk the organization is willing to accept. The CGEIT Review Manual 8th Edition highlights that the risk appetite is the primary consideration in developing risk management policies, as it guides decision-making and resource allocation.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"The enterprise's risk appetite is the primary consideration when developing a risk management policy. It defines the acceptable level of risk for IT-enabled investments and ensures that risk management practices align with the enterprise's strategic objectives and tolerance for uncertainty." (Approximate reference: Domain 3, Section on Risk Management Policy)

The risk appetite of the enterprise (option A) provides the foundation for determining how much risk is acceptable, which investments to pursue, and how to prioritize risk mitigation efforts.

Why not the other options?

B . Possible investment failures: While investment failures are a concern, they are a specific risk scenario, not the primary consideration for the policy, which should focus on the broader risk appetite.

C . Risk management framework: The framework is a tool to implement the policy, not the primary consideration for its development.

D . Value obtained with minimum risk: While value optimization is a goal, the policy must first be grounded in

the enterprise's risk appetite to balance risk and reward.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Risk Appetite and Policy Development.

ISACA CGEIT Study Guide, Chapter on Risk Management Policies.

Question: 651

Which of the following BEST helps to ensure that IT standards will be consistently applied across the enterprise?

A. Enterprise risk management (ERM) reviews.
B. Mandatory systems development training.
C. Business case reviews by the steering committee.
D. Established enterprise architecture (EA) practices.

Answer: D

Explanation:

Consistent application of IT standards across the enterprise is best achieved through a well-defined enterprise architecture (EA), which provides a blueprint for IT processes, technologies, and standards. The CGEIT Review Manual 8th Edition emphasizes that EA practices ensure standardization and alignment with enterprise objectives.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"Enterprise architecture provides a structured approach to defining and enforcing IT standards across the organization. By establishing common frameworks, policies, and guidelines, EA ensures consistency in the application of IT standards, reducing variability and enhancing interoperability." (Approximate reference: Domain 1, Section on Enterprise Architecture)

Established enterprise architecture practices (option D) provide a governance mechanism to enforce IT standards, ensuring that all IT initiatives adhere to predefined guidelines, thus promoting consistency.

Why not the other options?

A . Enterprise risk management (ERM) reviews: ERM focuses on identifying and mitigating risks, not on enforcing IT standards.

B . Mandatory systems development training: Training may improve skills but does not directly ensure consistent application of standards across the enterprise.

C . Business case reviews by the steering committee: Business case reviews focus on project approval and alignment, not on enforcing technical standards.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Enterprise Architecture and Standards.

ISACA CGEIT Study Guide, Chapter on Governance and EA.

Question: 652

An enterprise has learned of a new regulation that may impact delivery of one of its core technology services. Which of the following should be done FIRST?

A. Request an action plan from the risk team.
B. Determine whether the board wants to comply with the regulation.
C. Update the risk management framework.
D. Assess the risk associated with the new regulation.

Answer: D

Explanation:

A new regulation introduces a potential risk that must be assessed to understand its impact on the enterprise's operations and compliance obligations. The CGEIT Review Manual 8th Edition stresses that the first step in addressing new risks, such as regulations, is to conduct a risk assessment to evaluate their significance and implications.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"When a new regulation is identified, the first step is to assess the associated risk, including its potential impact on operations, compliance requirements, and the likelihood of enforcement. This assessment informs subsequent actions, such as developing mitigation plans or updating governance frameworks." (Approximate reference: Domain 3, Section on Risk Assessment)

Assessing the risk associated with the new regulation (option D) provides the enterprise with a clear understanding of the regulation's impact, enabling informed decisions about compliance, mitigation, or strategic adjustments.

Why not the other options?

A . Request an action plan from the risk team: An action plan is premature without first assessing the risk's scope and impact.

B . Determine whether the board wants to comply with the regulation: The board's decision on compliance should be informed by a risk assessment, not precede it.

C . Update the risk management framework: Updating the framework may be necessary later but is not the first step, as the specific risk must be understood first.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Risk Assessment and Regulatory Compliance.

ISACA CGEIT Study Guide, Chapter on Risk Management Processes.

Question: 653

Which of the following is the BEST way for an IT steering committee to monitor the adoption of a new enterprise IT strategy?

A. Implement service level agreements (SLAs).
B. Establish key performance indicators (KPIs).
C. Schedule ongoing audit reviews.
D. Establish key risk indicators (KRIs).

Answer: B

Explanation:

Monitoring the adoption of a new IT strategy requires measurable indicators that track progress and alignment with strategic objectives. The CGEIT Review Manual 8th Edition highlights that key performance indicators (KPIs) are the primary tool for monitoring strategy implementation, as they measure performance against defined goals.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"Key performance indicators (KPIs) are essential for monitoring the implementation and adoption of an IT strategy. KPIs provide measurable data on progress toward strategic objectives, enabling the IT steering committee to assess effectiveness and make informed adjustments." (Approximate reference: Domain 4, Section on Strategy Monitoring)

Establishing KPIs (option B) allows the IT steering committee to track the strategy's success, identify gaps, and

ensure alignment with enterprise goals, making it the best approach for monitoring adoption.
Why not the other options?
A . Implement service level agreements (SLAs): SLAs are operational agreements for service delivery, not strategic monitoring tools.
C . Schedule ongoing audit reviews: Audits provide assurance but are periodic and not designed for ongoing strategy monitoring.
D . Establish key risk indicators (KRIs): KRIs focus on risk exposure, not on measuring strategy adoption or performance.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Performance Measurement and Monitoring.
ISACA CGEIT Study Guide, Chapter on IT Strategy Implementation.

Question: 654

A regulator has expressed concerns about the timeliness of information reported from an enterprise.
Which of the following should be done FIRST to address this issue?
A. Assess the reporting delivery process.
B. Negotiate an exception process with the regulator.
C. Automate the reporting process.
D. Evaluate the implications of risk acceptance.

Answer: A

Explanation:

Concerns about the timeliness of reporting indicate a potential issue in the reporting process that must be investigated. The CGEIT Review Manual 8th Edition advises that the first step in addressing process-related issues is to assess the current process to identify bottlenecks, inefficiencies, or gaps. Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"When issues are raised regarding compliance or reporting, the first step is to assess the existing processes to identify root causes of deficiencies, such as delays or inaccuracies. This assessment provides the basis for designing improvements or corrective actions."
(Approximate reference: Domain 3, Section on
Compliance and Process Assessment)
Assessing the reporting delivery process (option A) allows the enterprise to pinpoint why reports are delayed, whether due to manual processes, data availability, or other factors, enabling targeted improvements.
Why not the other options?
B . Negotiate an exception process with the regulator: Negotiation is a reactive measure that does not address the root cause of untimely reporting.
C . Automate the reporting process: Automation may be a solution, but it is premature without understanding the current process's deficiencies.
D . Evaluate the implications of risk acceptance: Risk acceptance is a last resort and does not address the regulator's concern about timeliness.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Compliance and Process Improvement.
ISACA CGEIT Study Guide, Chapter on Regulatory Reporting.

Question: 655

Which of the following is the FIRST consideration for a CISO when implementing Zero Trust architecture?

A. Refining relevant business goals.
B. Limiting the number of privileged accounts.
C. Selecting a security framework that is relevant to the business.
D. Defining security projects to address identified control gaps.

Answer: A

Explanation:

Implementing a Zero Trust architecture requires alignment with business objectives to ensure that security measures support enterprise goals. The CGEIT Review Manual 8th Edition emphasizes that strategic initiatives, including security architectures, must start with a clear understanding of business goals to ensure relevance and value.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"Security initiatives, such as the adoption of new architectures like Zero Trust, must begin with an understanding of business goals and objectives. Refining relevant business goals ensures that security measures are aligned with enterprise priorities and deliver value." (Approximate reference: Domain 3, Section on Security Strategy Alignment)

Refining relevant business goals (option A) ensures that the Zero Trust implementation focuses on protecting critical assets and processes that are most important to the business, setting the stage for subsequent technical and operational decisions.

Why not the other options?

B . Limiting the number of privileged accounts: This is a tactical measure within Zero Trust but not the first consideration, as it depends on understanding business priorities.

C . Selecting a security framework that is relevant to the business: Framework selection follows the definition of business goals, as the framework must support those goals.

D . Defining security projects to address identified control gaps: Projects are defined after identifying business goals and assessing current controls.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Security Strategy and Alignment.

ISACA CGEIT Study Guide, Chapter on Security Governance.

Question: 656

An enterprise plans to implement a business intelligence tool with data sources from various enterprise applications. Which of the following is the GREATEST challenge to implementation?

A. Interface issues between enterprise and business intelligence applications.
B. The need for staff to be trained on the new business intelligence tool.
C. Large volumes of data fed from enterprise applications.
D. Data definition and mapping sources from applications.

Answer: D

Explanation:

Implementing a business intelligence (BI) tool requires integrating data from multiple enterprise applications, and the greatest challenge is often ensuring that data definitions and mappings are consistent and accurate. The CGEIT Review Manual 8th Edition notes that data integration, particularly defining and mapping data sources, is a critical hurdle in BI projects due to varying data formats, structures, and semantics across systems.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"The success of business

intelligence initiatives depends heavily on the quality and consistency of data. Data definition and mapping from disparate enterprise applications is often the greatest challenge, as inconsistencies in data formats, structures, and meanings can lead to inaccurate insights and project delays." (Approximate reference: Domain 5, Section on Data Management for BI)

Data definition and mapping sources from applications (option D) is the greatest challenge because it involves resolving differences in how data is structured, labeled, and interpreted across systems, which is foundational to BI success.

Why not the other options?

A . Interface issues between enterprise and BI applications: Interface issues are technical but typically less challenging than data mapping, as they can often be addressed with middleware or APIs.

B . The need for staff to be trained on the new BI tool: Training is a manageable challenge that occurs post-implementation and is not as critical as data integration.

C . Large volumes of data fed from enterprise applications: While large data volumes pose a challenge, modern BI tools are designed to handle big data, making data mapping the more significant issue.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on Business Intelligence and Data Management.

ISACA CGEIT Study Guide, Chapter on BI Implementation.

Question: 657

Which of the following is the GREATEST advantage of earned value management when used for evaluating benefits from the implementation of blockchain projects for IT contracts management? A. It automates project progress reporting to business executives.

B. It provides a measure of project progress that is easy to understand.

C. It eliminates potential risks related to project earnings.

D. It enables accurate forecasts of the number of blocks to be completed.

Answer: B

Explanation:

Earned value management (EVM) is a project management technique that integrates scope, schedule, and cost to measure project performance and progress. The CGEIT Review Manual 8th Edition highlights that EVM's greatest advantage is its ability to provide a clear, quantifiable measure of project progress that stakeholders can easily understand.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"Earned value management provides a standardized, easy-to-understand measure of project progress by comparing planned value, earned value, and actual costs. This enables stakeholders to assess whether a project, such as a blockchain implementation, is on track to deliver expected benefits." (Approximate reference: Domain 5, Section on Project Performance Measurement)

Providing a measure of project progress that is easy to understand (option B) is the greatest advantage, as EVM offers clear metrics (e.g., cost variance, schedule variance) that help executives and stakeholders gauge the success of blockchain projects for IT contracts management.

Why not the other options?

A . It automates project progress reporting to business executives: EVM is not an automated reporting tool; it requires data collection and analysis.

C . It eliminates potential risks related to project earnings: EVM identifies variances but does not eliminate risks.

D . It enables accurate forecasts of the number of blocks to be completed: EVM measures progress in terms

of value, not specific technical outputs like blockchain blocks.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on Earned Value Management.

ISACA CGEIT Study Guide, Chapter on Project Benefits Tracking.

Question: 658

Due to budget cuts, IT has been forced to limit service offerings in the portfolio. There has been significant resistance from business leaders to this decision. Which of the following is the BEST way for the CIO to find a solution that is aligned with business objectives?

A. Engage an external consultant to document IT's alignment with the business.
B. Perform a cost-benefit analysis and communicate results.
C. Reallocate budget from maintenance projects in the portfolio.
D. Collaborate with the business to prioritize the IT portfolio.

Answer: D

Explanation:

Resistance from business leaders indicates a lack of alignment between IT decisions and business priorities. The CGEIT Review Manual 8th Edition emphasizes that collaboration with business stakeholders is critical to ensure that IT portfolio decisions reflect business objectives, especially when resources are constrained.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"When faced with resource constraints, the CIO should collaborate with business stakeholders to prioritize the IT portfolio based on business objectives. This ensures that limited resources are allocated to initiatives that deliver the greatest value and alignment with enterprise goals." (Approximate reference: Domain 4, Section on Portfolio Management)

Collaborating with the business to prioritize the IT portfolio (option D) directly addresses the resistance by involving business leaders in decision-making, ensuring that IT services align with their priorities and reducing conflict.

Why not the other options?

A . Engage an external consultant to document IT's alignment with the business: An external consultant may provide insights but does not address the immediate need for collaboration and buyin from business leaders.

B . Perform a cost-benefit analysis and communicate results: While analysis is useful, it does not involve business leaders in the prioritization process, which is key to resolving resistance.

C . Reallocate budget from maintenance projects in the portfolio: Reallocation is a unilateral action that may exacerbate resistance if not done in collaboration with the business.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on IT Portfolio Management.

ISACA CGEIT Study Guide, Chapter on Business-IT Alignment.

Question: 659

What should be the FIRST action of a new CIO when considering an IT governance framework for an enterprise?

A. Develop an IT balanced scorecard to monitor and track IT performance.
B. Verify stakeholder sponsorship of the IT governance initiative.
C. Understand corporate culture and IT's role in providing business value.

D. Understand critical IT processes to define the scope of the IT governance framework.

Answer: C

Explanation:

A new CIO must first understand the enterprise's context, including its corporate culture and how IT contributes to business value, to ensure that the IT governance framework is relevant and effective. The CGEIT Review Manual 8th Edition stresses that understanding the organizational context is the foundational step for governance initiatives.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"Before designing an IT governance framework, the CIO must understand the enterprise's corporate culture, business objectives, and the role of IT in delivering value. This ensures that the governance framework is tailored to the organization's unique needs and context." (Approximate reference: Domain 1, Section on Governance Framework Development)

Understanding corporate culture and IT's role in providing business value (option C) sets the stage for designing a governance framework that aligns with the enterprise's goals and is accepted by stakeholders.

Why not the other options?

A . Develop an IT balanced scorecard to monitor and track IT performance: A balanced scorecard is a performance management tool, not the first step in governance framework development.

B . Verify stakeholder sponsorship of the IT governance initiative: Sponsorship is important but follows understanding the organizational context, as the CIO needs to know what stakeholders value. D . Understand critical IT processes to define the scope of the IT governance framework: Process understanding is a subsequent step that builds on the broader organizational context.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Organizational Context for Governance.

ISACA CGEIT Study Guide, Chapter on IT Governance Framework Design.

Question: 660

A board of directors is concerned with the total cost of IT. Which of the following is MOST important for the CIO to include in an explanation to the board?

A. A summary of benefits that will be achieved once key IT initiatives are completed.
B. A mapping of IT employee roles to the balanced scorecard.
C. A benchmark of IT employee salary costs against comparable organizations.
D. A breakdown of operational versus capital expenditures.

Answer: D

Explanation:

The board's concern about the total cost of IT requires a clear explanation of how IT spending is structured. The CGEIT Review Manual 8th Edition notes that providing a breakdown of operational versus capital expenditures is critical to helping stakeholders understand IT costs and their alignment with business value.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"When addressing concerns about IT costs, the CIO should provide a clear breakdown of operational expenditures (e.g., maintenance, salaries) versus capital expenditures (e.g., new systems, infrastructure). This transparency helps the board understand cost drivers and their contribution to business value." (Approximate reference: Domain 5, Section on Cost Management)

A breakdown of operational versus capital expenditures (option D) directly addresses the board's concern by showing how IT funds are allocated, distinguishing between ongoing costs and investments in new capabilities.

Why not the other options?

A . A summary of benefits that will be achieved once key IT initiatives are completed: While benefits are important, they do not directly address the total cost concern, which requires cost transparency first.

B . A mapping of IT employee roles to the balanced scorecard: This is a performance management tool, not directly relevant to explaining total IT costs.

C . A benchmark of IT employee salary costs against comparable organizations: Benchmarking salaries is a narrow focus and does not provide a comprehensive view of total IT costs. Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on IT Cost Management.

ISACA CGEIT Study Guide, Chapter on Cost Transparency.

Question: 661

Which of the following is MOST important to ensure that IT project selections meet the enterprise's business requirements?

A. Development of an enterprise architecture (EA).
B. Business participation in the selection of IT projects.
C. Implementation of project stage gates.
D. Creation of thorough business cases prior to IT project selection.

Answer: B

Explanation:

Ensuring that IT project selections meet business requirements requires direct involvement of business stakeholders to align projects with enterprise goals. The CGEIT Review Manual 8th Edition emphasizes that business participation in project selection is critical to achieving strategic alignment. Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"Business participation in the selection of IT projects is essential to ensure that projects are aligned with enterprise business requirements and deliver value. Engaging business stakeholders in the decisionmaking process fosters alignment and prioritization of initiatives that support strategic goals." (Approximate reference: Domain 4, Section on Project Portfolio Management)

Business participation in the selection of IT projects (option B) ensures that projects are chosen based on business needs, increasing the likelihood of delivering value and meeting requirements. Why not the other options?

A . Development of an enterprise architecture (EA): EA provides a framework but does not directly ensure business requirements are met in project selection.

C . Implementation of project stage gates: Stage gates control project execution, not the initial selection process.

D . Creation of thorough business cases prior to IT project selection: Business cases are important, but they are a tool used during selection, which requires business participation to be effective.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Business-IT Alignment in Project Selection.

ISACA CGEIT Study Guide, Chapter on Project Portfolio Governance.

Question: 662

Despite an adequate training budget, IT staff are not keeping skills current with emerging technologies critical

to the business. Which of the following is the BEST way for the enterprise to address this situation?

A. Provide incentives for IT staff to attend outside conferences and training.
B. Require human resources (HR) to recruit new talent using an established IT skills matrix.
C. Create a standard-setting center of excellence for IT.
D. Establish an agreed-upon skills development plan with each employee.

Answer: D

Explanation:

When IT staff fail to keep skills current despite available training, the issue often lies in a lack of targeted, individualized development plans. The CGEIT Review Manual 8th Edition recommends creating personalized skills development plans to ensure that training aligns with both individual and organizational needs.
Extract from CGEIT Review Manual 8th Edition (Domain 2: IT Resources):"To address skill gaps, enterprises should establish individualized skills development plans that align employee training with emerging technologies and business needs. These plans ensure that training is relevant, targeted, and effectively utilized to maintain a skilled workforce." (Approximate reference: Domain 2, Section on Skills Development)
Establishing an agreed-upon skills development plan with each employee (option D) ensures that training is tailored to the specific technologies critical to the business and that employees are accountable for skill development.
Why not the other options?
A . Provide incentives for IT staff to attend outside conferences and training: Incentives may encourage participation but do not ensure that training addresses specific skill gaps.
B . Require human resources (HR) to recruit new talent using an established IT skills matrix: Recruiting is a last resort and does not address the current staff's skill deficiencies.
C . Create a standard-setting center of excellence for IT: A center of excellence may set standards but does not directly address individual skill development.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 2: IT Resources, Section on Workforce Development.
ISACA CGEIT Study Guide, Chapter on IT Skills Management.

Question: 663

An enterprise's IT director is concerned that the chair of the IT steering committee is stealing confidential company information. Which of the following is the IT director's BEST course of action?

A. File a report with the local law enforcement agency.
B. Report the concern to the ethics hotline.
C. Discuss the concern with the chair directly.
D. Conduct an investigation to substantiate the chair's activities.

Answer: B

Explanation:

Concerns about unethical behavior, such as stealing confidential information, should be reported through established ethical reporting mechanisms to ensure impartiality and compliance with governance policies. The CGEIT Review Manual 8th Edition advises using ethics hotlines or similar channels to handle allegations of misconduct.
Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"Allegations of unethical behavior, including the misuse of confidential information, should be reported through the

enterprise's ethics hotline or designated reporting channel. This ensures that concerns are handled impartially, in accordance with governance policies, and with appropriate escalation to senior management or the board." (Approximate reference: Domain 1, Section on Ethical Governance)

Reporting the concern to the ethics hotline (option B) is the best course of action, as it follows governance protocols, protects the IT director from retaliation, and ensures an independent investigation.

Why not the other options?

A . File a report with the local law enforcement agency: Involving law enforcement is premature without evidence and bypasses internal governance processes.

C . Discuss the concern with the chair directly: Confronting the chair risks escalation and lacks impartiality, potentially compromising the investigation.

D . Conduct an investigation to substantiate the chair's activities: The IT director should not conduct an investigation personally, as this could compromise objectivity and governance protocols.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Ethics and Compliance.

ISACA CGEIT Study Guide, Chapter on Governance and Ethical Behavior.

Question: 664

Which of the following should be the PRIMARY consideration when implementing IT governance in a small, newly established organization?

A. Assigning a budget for IT governance applications.
B. Defining IT project management methodology.
C. Approving enterprise architecture (EA) and standards.
D. Assigning IT roles and responsibilities.

Answer: D

Explanation:

In a small, newly established organization, the foundation of IT governance lies in clearly defining roles and responsibilities to ensure accountability and decision-making clarity. The CGEIT Review Manual 8th Edition emphasizes that assigning roles and responsibilities is a critical first step in governance, especially for organizations with limited resources.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"In small or newly established organizations, the primary consideration for IT governance is to assign clear IT roles and responsibilities. This establishes accountability, clarifies decision-making authority, and lays the foundation for effective governance processes." (Approximate reference: Domain 1, Section on Governance Structure)

Assigning IT roles and responsibilities (option D) ensures that the organization has a clear structure for IT decision-making, which is essential before addressing budgets, methodologies, or architectures.

Why not the other options?

A . Assigning a budget for IT governance applications: Budgeting is important but secondary to establishing governance roles, as roles define who manages the budget.

B . Defining IT project management methodology: Methodologies are operational and follow the establishment of governance structures.

C . Approving enterprise architecture (EA) and standards: EA is a subsequent step that requires governance roles to be in place for effective decision-making.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Governance

Roles and Responsibilities.
ISACA CGEIT Study Guide, Chapter on Governance in Small Organizations.

Question: 665

The board of an enterprise has decided to implement an emerging technology, and employees are extremely concerned about the unknown future of the company. What should be the CIO's PRIMARY responsibility in addressing these concerns?

A. Develop and communicate new performance measures.
B. Define new roles and responsibilities for IT staff.
C. Initiate IT workforce training on the new technology.
D. Define and communicate a new IT strategy.

Answer: D

Explanation:

Employee concerns about the future due to an emerging technology stem from uncertainty about the organization's direction. The CGEIT Review Manual 8th Edition emphasizes that the CIO's primary responsibility in such scenarios is to define and communicate a clear IT strategy to provide direction and reassurance.
Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"When adopting emerging technologies, the CIO's primary responsibility is to define and communicate an IT strategy that aligns with the enterprise's goals and addresses stakeholder concerns. Clear communication of the strategy reduces uncertainty and fosters confidence in the organization's direction." (Approximate reference: Domain 4, Section on Strategic Communication)
Defining and communicating a new IT strategy (option D) addresses employee concerns by clarifying how the technology supports business goals, how it will be implemented, and its impact on the workforce.
Why not the other options?
A . Develop and communicate new performance measures: Performance measures are operational and do not directly address concerns about the company's future.
B . Define new roles and responsibilities for IT staff: Roles may need redefinition, but this is a secondary step after communicating the strategy.
C . Initiate IT workforce training on the new technology: Training is important but does not address broader concerns about the company's direction.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on IT Strategy Communication.
ISACA CGEIT Study Guide, Chapter on Managing Change in IT Strategy.

Question: 666

An enterprise is considering outsourcing non-core IT processes. Which of the following should be the FIRST step?

A. Update resource allocation policies.
B. Issue a formal request for proposal (RFP) to outsourcing vendors.
C. Establish service-level metrics for outsourced activities.
D. Conduct a cost-benefit analysis for outsourcing.

Answer: D

Explanation:

Outsourcing decisions require a clear understanding of the financial and operational implications. The CGEIT Review Manual 8th Edition advises that conducting a cost-benefit analysis is the first step to evaluate whether outsourcing non-core IT processes aligns with enterprise objectives.
Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"Before outsourcing IT processes, the enterprise should conduct a cost-benefit analysis to assess the financial, operational, and strategic implications. This analysis determines whether outsourcing delivers value and supports business objectives." (Approximate reference: Domain 5, Section on Outsourcing Decisions)
Conducting a cost-benefit analysis for outsourcing (option D) provides the data needed to make an informed decision, comparing costs, risks, and benefits of outsourcing versus in-house management. Why not the other options?
A . Update resource allocation policies: Policy updates follow the decision to outsource, based on the analysis.
B . Issue a formal request for proposal (RFP) to outsourcing vendors: Issuing an RFP is premature without confirming that outsourcing is viable.
C . Establish service-level metrics for outsourced activities: Metrics are defined after deciding to outsource and selecting a vendor.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on Outsourcing and Value Delivery.
ISACA CGEIT Study Guide, Chapter on Outsourcing Decisions.

Question: 667

When establishing a comprehensive approach for analyzing IT risk in an international, multi-division enterprise, it is MOST important to ensure:

A. Risk management methodologies are aligned with local best practices.
B. IT senior managers perform the analysis.
C. Risk scenarios are compartmentalized by division.
D. A consistent risk management methodology is used.

Answer: D

Explanation:

In an international, multi-division enterprise, a consistent risk management methodology ensures that risks are analyzed uniformly across divisions, enabling comparability and enterprise-wide prioritization. The CGEIT Review Manual 8th Edition emphasizes the importance of a standardized approach to risk management in complex organizations.
Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"In multi-division or international enterprises, a consistent risk management methodology is critical to ensure that risks are assessed and prioritized uniformly across the organization. This enables aggregation of risks and alignment with enterprise-wide objectives." (Approximate reference: Domain 3, Section on Enterprise Risk Management)
Using a consistent risk management methodology (option D) ensures that all divisions apply the same criteria, processes, and tools, facilitating a cohesive risk profile and effective decision-making. Why not the other options?
A . Risk management methodologies are aligned with local best practices: Local alignment may lead to inconsistencies across divisions, undermining enterprise-wide risk management.
B . IT senior managers perform the analysis: While senior managers may be involved, the methodology itself is more important than who performs the analysis.

C . Risk scenarios are compartmentalized by division: Compartmentalization may prevent a holistic view of enterprise risks, reducing effectiveness.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Risk Management Methodologies.

ISACA CGEIT Study Guide, Chapter on Enterprise Risk Management.

Question: 668

Which of the following should be the MOST essential consideration when outsourcing IT services?

A. Identification of core and non-core business processes.
B. Compliance with enterprise architecture (EA).
C. Alignment with existing human resources (HR) policies and practices.
D. Adoption of a diverse vendor selection process.

Answer: A

Explanation:

Outsourcing IT services requires a clear distinction between core and non-core processes to ensure that strategic capabilities are retained in-house while non-core activities are outsourced. The CGEIT Review Manual 8th Edition highlights that identifying core and non-core processes is the most essential consideration for outsourcing decisions.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"The most critical consideration in outsourcing IT services is identifying core and non-core business processes. Core processes, which provide competitive advantage, should typically be retained, while non-core processes can be outsourced to improve efficiency and focus on strategic priorities." (Approximate reference: Domain 5, Section on Outsourcing Strategy)

Identification of core and non-core business processes (option A) ensures that outsourcing aligns with the enterprise's strategic goals and avoids compromising critical capabilities.

Why not the other options?

B . Compliance with enterprise architecture (EA): EA compliance is important but secondary to determining what processes should be outsourced.

C . Alignment with existing human resources (HR) policies and practices: HR alignment is operational and less critical than strategic process identification.

D . Adoption of a diverse vendor selection process: Vendor selection follows the decision to outsource and is not the primary consideration.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on Outsourcing and Core Competencies.

ISACA CGEIT Study Guide, Chapter on Strategic Outsourcing.

Question: 669

A CIO engages a consulting firm to conduct a benchmark analysis of the organization's IT governance framework against industry best practices. Several recommendations to improve the maturity of the framework are identified. Which of the following should be the CIO's NEXT course of action?

A. Evaluate the feasibility of the recommendations.
B. Obtain approval from the IT steering committee to implement the recommendations.
C. Develop a plan to integrate the recommendations.
D. Appoint a project manager to implement the recommendations.

Answer: A

Explanation:

After receiving recommendations to improve the IT governance framework, the CIO must assess their feasibility to ensure they are practical and aligned with the enterprise's resources and goals. The CGEIT Review Manual 8th Edition advises evaluating the feasibility of recommendations as the next step to prioritize and plan implementation.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"Following a benchmark analysis, the CIO should evaluate the feasibility of recommendations, considering factors such as cost, resource availability, organizational readiness, and alignment with strategic objectives. This assessment informs the prioritization and planning of implementation efforts." (Approximate reference: Domain 1, Section on Governance Framework Improvement)

Evaluating the feasibility of the recommendations (option A) ensures that the CIO selects recommendations that are viable and beneficial, setting the stage for planning and approval. Why not the other options?

B . Obtain approval from the IT steering committee to implement the recommendations: Approval is needed but follows feasibility assessment to ensure informed decision-making.

C . Develop a plan to integrate the recommendations: Planning is premature without confirming which recommendations are feasible.

D . Appoint a project manager to implement the recommendations: Appointing a project manager is a later step, after feasibility and planning.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Framework Benchmarking and Improvement.

ISACA CGEIT Study Guide, Chapter on Governance Framework Enhancement.

Question: 670

Which of the following should be the CIO's GREATEST consideration when making changes to the IT strategy?

A. Have key stakeholders been consulted?
B. Has the impact to the enterprise architecture (EA) been assessed?
C. Have IT risk metrics been adjusted?
D. Has the investment portfolio been revised?

Answer: B

Explanation:

Changes to the IT strategy must consider their impact on the enterprise architecture (EA), as the EA defines the structure and standards that enable strategy execution. The CGEIT Review Manual 8th Edition highlights that assessing EA impact is the greatest consideration to ensure that strategic changes are feasible and sustainable.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"When modifying the IT strategy, the CIO's greatest consideration is assessing the impact on the enterprise architecture, as the EA provides the blueprint for IT capabilities, processes, and standards.

Misalignment with EA can lead to implementation challenges and reduced effectiveness." (Approximate reference: Domain 4, Section on Strategy and EA Alignment)

Assessing the impact to the enterprise architecture (option B) ensures that the IT strategy leverages existing capabilities and addresses any architectural gaps, making it the most critical consideration. Why not the other options?

A . Have key stakeholders been consulted?: Stakeholder consultation is important but secondary to ensuring the strategy is technically feasible via EA alignment.

C . Have IT risk metrics been adjusted?: Risk metrics are adjusted as part of risk management, not the primary concern for strategy changes.

D . Has the investment portfolio been revised?: Portfolio revision follows strategy and EA alignment to ensure investments support the updated strategy.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Enterprise Architecture and Strategy.

ISACA CGEIT Study Guide, Chapter on IT Strategy Updates.

Question: 671

Which of the following should be done FIRST when preparing to migrate patient records to a cloud service provider?

A. Review the current data governance policy.
B. Update the enterprise architecture (EA).
C. Revise the risk management framework.
D. Define the service level agreement (SLA).

Answer: A

Explanation:

Migrating patient records to a cloud provider involves sensitive data, making data governance a critical first step to ensure compliance and security. The CGEIT Review Manual 8th Edition emphasizes that reviewing the data governance policy is the first action to align migration with data protection and regulatory requirements.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"When migrating sensitive data, such as patient records, to a cloud environment, the first step is to review the current data governance policy to ensure that data classification, security, and compliance requirements are addressed. This informs subsequent actions, such as SLAs and risk management." (Approximate reference: Domain 3, Section on Data Governance and Cloud Migration)

Reviewing the current data governance policy (option A) ensures that the migration adheres to policies on data privacy, security, and regulatory compliance, particularly for sensitive patient records.

Why not the other options?

B . Update the enterprise architecture (EA): EA updates may be needed but follow governance review to ensure alignment with data policies.

C . Revise the risk management framework: Risk framework revision is premature without understanding governance requirements.

D . Define the service level agreement (SLA): SLAs are defined after governance and risk considerations are addressed.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Data Governance and Cloud Security.

ISACA CGEIT Study Guide, Chapter on Cloud Migration Governance.

Question: 672

Which of the following is MOST important to effectively incorporate innovation and emerging technologies

into an enterprise's IT strategy?

A. Implementing new technologies based on maturity roadmaps according to reputable consulting entities.
B. Maintaining an IT strategy based on traditional technologies, supplemented by objectives for innovation.
C. Establishing a formal innovation management process that involves IT and business stakeholders.
D. Performing quarterly feedback reviews with focus groups representing the enterprise's customer base.

Answer: C

Explanation:

Incorporating innovation and emerging technologies into the IT strategy requires a structured process that engages both IT and business stakeholders to ensure alignment and value delivery. The CGEIT Review Manual 8th Edition highlights that a formal innovation management process is critical to effectively integrate new technologies.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"To effectively incorporate innovation and emerging technologies, enterprises should establish a formal innovation management process that involves IT and business stakeholders. This process ensures that new technologies are evaluated, prioritized, and aligned with business objectives." (Approximate reference: Domain 4, Section on Innovation Management)

Establishing a formal innovation management process that involves IT and business stakeholders (option C) fosters collaboration, ensures strategic alignment, and drives successful adoption of emerging technologies.

Why not the other options?

A . Implementing new technologies based on maturity roadmaps according to reputable consulting entities: Relying on external roadmaps may not align with the enterprise's specific needs.

B . Maintaining an IT strategy based on traditional technologies, supplemented by objectives for innovation: This approach limits innovation by prioritizing traditional technologies.

D . Performing quarterly feedback reviews with focus groups representing the enterprise's customer base: Customer feedback is valuable but not the primary mechanism for strategic technology integration.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Innovation and Technology Strategy.

ISACA CGEIT Study Guide, Chapter on Innovation Management.

Question: 673

An enterprise's IT department has been operating independently without regard to business concerns, leading to misalignment between business and IT. The BEST way to establish alignment would be to require:

A. Business to help define IT goals.
B. IT and business to define risks.
C. Business to fund IT services.
D. IT to define business objectives.

Answer: A

Explanation:

Misalignment between IT and business stems from a lack of collaboration in setting goals. The CGEIT Review Manual 8th Edition emphasizes that business involvement in defining IT goals is the best way to ensure alignment, as it ensures IT supports business priorities.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"To achieve alignment between IT and business, the business must actively participate in defining IT goals to ensure that IT initiatives support enterprise objectives. This collaborative approach bridges the gap between IT operations and business needs." (Approximate reference: Domain 4, Section on Business- IT Alignment)

Requiring the business to help define IT goals (option A) fosters collaboration and ensures that IT priorities reflect business needs, addressing the misalignment.

Why not the other options?

B . IT and business to define risks: Risk definition is important but does not directly address goal alignment.

C . Business to fund IT services: Funding is a resource issue, not a solution to strategic misalignment.

D . IT to define business objectives: IT defining business objectives reverses the proper alignment, as business objectives should drive IT.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Strategic Alignment.

ISACA CGEIT Study Guide, Chapter on Business-IT Collaboration.

Question: 674

Which of the following is the PRIMARY objective of a data protection impact assessment?

A. To identify and analyze how data privacy might be affected by business processes.
B. To evaluate the quality and integrity of personal data stored in an enterprise.
C. To estimate the value created by personal data as it progresses through its life cycle.
D. To ensure key business processes and related data interfaces are documented.

Answer: A

Explanation:

A data protection impact assessment (DPIA) is designed to identify and mitigate risks to data privacy. The CGEIT Review Manual 8th Edition states that the primary objective of a DPIA is to analyze how business processes affect data privacy, particularly for personal data.

Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"The primary objective of a data protection impact assessment is to identify and analyze how business processes, systems, or projects may impact the privacy of personal data. This helps ensure compliance with data protection regulations and mitigates privacy risks." (Approximate reference: Domain 3, Section on Data Privacy and Compliance)

Identifying and analyzing how data privacy might be affected by business processes (option A) is the core purpose of a DPIA, aligning with regulatory requirements like GDPR.

Why not the other options?

B . To evaluate the quality and integrity of personal data stored in an enterprise: Data quality is a separate concern, not the focus of a DPIA.

C . To estimate the value created by personal data as it progresses through its life cycle: Value estimation is a business analysis, not a DPIA objective.

D . To ensure key business processes and related data interfaces are documented: Documentation may be a byproduct, but it is not the primary objective.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Data Protection Impact Assessments.

ISACA CGEIT Study Guide, Chapter on Privacy and Compliance.

Question: 675

An enterprise wants to implement metrics to monitor the performance of its IT portfolio. Whose input is

MOST important to consider when establishing these metrics?

A. Project management office (PMO).
B. IT executives.
C. The chief executive officer (CEO).
D. Business unit stakeholders.

Answer: D

Explanation:

IT portfolio performance metrics must reflect the value delivered to the business, making business unit stakeholders' input critical. The CGEIT Review Manual 8th Edition emphasizes that business stakeholders are the primary source for defining metrics that align with business objectives.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"When establishing metrics to monitor IT portfolio performance, the input of business unit stakeholders is most important, as they define the business objectives and value expectations that the IT portfolio must deliver." (Approximate reference: Domain 5, Section on Performance Metrics)

Considering the input of business unit stakeholders (option D) ensures that metrics measure outcomes that matter to the business, such as revenue growth, customer satisfaction, or operational efficiency.

Why not the other options?

A . Project management office (PMO): The PMO focuses on project execution, not business value definition.

B . IT executives: IT executives provide technical input, but business stakeholders define value.

C . The chief executive officer (CEO): The CEO may set high-level goals, but business units provide detailed requirements.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on Portfolio Performance Measurement.

ISACA CGEIT Study Guide, Chapter on Business Value Metrics.

Question: 676

Which of the following provides an enterprise with the BEST understanding of the value proposition for employing a new cloud service?

A. Key risk indicators (KRIs).
B. Service level agreements (SLAs).
C. Return on investment (ROI).
D. Customer satisfaction surveys.

Answer: C

Explanation:

The value proposition of a new cloud service is best understood through a financial metric like return on investment (ROI), which quantifies the benefits relative to costs. The CGEIT Review Manual 8th Edition highlights ROI as a key tool for evaluating the value of IT investments.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"Return on investment (ROI) is a critical metric for understanding the value proposition of IT initiatives, such as adopting a new cloud service. ROI compares the financial benefits of the initiative to its costs, providing a clear measure of value delivered." (Approximate reference: Domain 5, Section on Value Measurement)

Return on investment (option C) provides a comprehensive view of the cloud service's financial benefits, operational improvements, and strategic value, making it the best tool for understanding the value

proposition.

Why not the other options?

A . Key risk indicators (KRIs): KRIs focus on risk exposure, not value delivery.

B . Service level agreements (SLAs): SLAs define performance expectations but do not quantify overall value.

D . Customer satisfaction surveys: Surveys measure user experience, not the full financial or strategic value.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on ROI and Value Assessment.

ISACA CGEIT Study Guide, Chapter on IT Investment Evaluation.

Question: 677

Which of the following is MOST important to have in place to ensure a business continuity plan (BCP) can be executed?

A. Defined roles.
B. Replicated systems.
C. A risk register.
D. Budget allocation.

Answer: A

Explanation:

A business continuity plan (BCP) relies on clear roles and responsibilities to ensure effective execution during a disruption. The CGEIT Review Manual 8th Edition emphasizes that defined roles are the most critical component for BCP success, as they ensure accountability and coordination. Extract from CGEIT Review Manual 8th Edition (Domain 3: Risk Optimization):"The most important element for executing a business continuity plan is the definition of roles and responsibilities. Clear roles ensure that all stakeholders know their duties during a disruption, enabling rapid and coordinated response." (Approximate reference: Domain 3, Section on Business Continuity Planning) Defined roles (option A) are essential to ensure that the BCP is actionable, with individuals assigned to specific tasks, such as communication, recovery, or coordination.

Why not the other options?

B . Replicated systems: Systems are important but useless without people to manage them during a crisis.

C . A risk register: A risk register identifies risks but does not ensure BCP execution.

D . Budget allocation: Funding supports BCP development but is not the most critical for execution.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 3: Risk Optimization, Section on Business Continuity and Disaster Recovery.

ISACA CGEIT Study Guide, Chapter on BCP Execution.

Question: 678

Which of the following should be considered FIRST when migrating data to a cloud environment?

A. Disaster recovery plan (DRP).
B. Skills matrix.
C. Information architecture.
D. Data structure.

Answer: C

Explanation:

Migrating data to a cloud environment requires a clear understanding of the information architecture to ensure data is organized, accessible, and secure. The CGEIT Review Manual 8th Edition notes that information architecture is the first consideration to align data migration with enterprise needs.
Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"When migrating data to a cloud environment, the first consideration is the information architecture, which defines how data is structured, stored, and accessed. This ensures that the migration supports business processes and complies with governance requirements." (Approximate reference: Domain 4, Section on Cloud Migration Strategy)
Considering the information architecture (option C) ensures that the cloud environment supports the enterprise's data needs, security policies, and integration requirements.
Why not the other options?
A . Disaster recovery plan (DRP): DRP is important but follows architecture design to ensure recovery aligns with data organization.
B . Skills matrix: Skills are a resource consideration, not the first step in data migration.
D . Data structure: Data structure is a component of information architecture, which is the broader consideration.
Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Information Architecture and Cloud.
ISACA CGEIT Study Guide, Chapter on Cloud Migration Planning.

Question: 679

An executive management team has determined the need to implement an IT governance framework, beginning with the maturity assessment process. The PRIMARY purpose for maturity assessment is to:

A. Benchmark IT performance.
B. Identify gaps in performance.
C. Support impact analysis.
D. Identify gaps in capability.

Answer: D

Explanation:
A maturity assessment evaluates the current state of IT governance processes to identify gaps in capability that need improvement. The CGEIT Review Manual 8th Edition states that the primary purpose of a maturity assessment is to identify capability gaps to guide governance framework enhancements.
Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"The primary purpose of a maturity assessment is to identify gaps in IT governance capabilities, such as processes, skills, or controls, relative to desired maturity levels. This enables the enterprise to prioritize improvements and enhance governance effectiveness." (Approximate reference: Domain 1, Section on Maturity Assessment)
Identifying gaps in capability (option D) focuses on assessing the maturity of governance processes and determining where enhancements are needed to achieve desired outcomes.
Why not the other options?
A . Benchmark IT performance: Benchmarking compares performance, not capability maturity.
B . Identify gaps in performance: Performance gaps are a secondary outcome, while capability gaps are the primary focus.
C . Support impact analysis: Impact analysis is not the primary purpose of maturity assessments. Reference:
ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Governance Maturity Assessment.
ISACA CGEIT Study Guide, Chapter on IT Governance Maturity.

Question: 680

Which of the following is the BEST indicator of effective IT governance?

A. Regulatory authorities have given a favorable report on IT controls.
B. Executive management is involved in important IT decisions and activities.
C. The chief information security officer (CISO) reports to a board member.
D. IT management is proactive in reporting IT project status to executive management.

Answer: B

Explanation:

Effective IT governance ensures that IT aligns with enterprise objectives, and a key indicator is the active involvement of executive management in IT decision-making. The CGEIT Review Manual 8th Edition emphasizes that executive management's engagement in IT decisions demonstrates strong governance, as it ensures strategic alignment, accountability, and oversight.

Extract from CGEIT Review Manual 8th Edition (Domain 1: Governance of Enterprise IT):"Effective IT governance is best indicated by the active involvement of executive management in important IT decisions and activities. This engagement ensures that IT initiatives are aligned with business objectives, risks are managed appropriately, and value is delivered to the enterprise." (Approximate reference: Domain 1, Section on Governance Roles and Responsibilities)

Executive management's involvement (option B) reflects a governance structure where IT is integrated into strategic planning, ensuring decisions support business goals and foster accountability at the highest levels.

Why not the other options?

A . Regulatory authorities have given a favorable report on IT controls: While a favorable regulatory report indicates compliance, it is a narrow measure and does not encompass the broader aspects of governance, such as strategic alignment or value delivery.

C . The chief information security officer (CISO) reports to a board member: The CISO's reporting structure is a specific governance element but not the best indicator of overall IT governance effectiveness, as it focuses only on security.

D . IT management is proactive in reporting IT project status to executive management: Proactive reporting is a good practice but is a subset of governance activities, less critical than executive management's direct involvement in decision-making.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 1: Governance of Enterprise IT, Section on Governance Roles and Executive Involvement.

ISACA CGEIT Study Guide, Chapter on IT Governance Indicators.

Question: 681

An enterprise will be adopting wearable technology to improve business performance. Which of the following is the BEST way for the CIO to validate IT's preparedness for this initiative?

A. Request an enterprise architecture (EA) review.
B. Perform a baseline business value assessment.
C. Request reprioritization of the IT portfolio.
D. Identify the penalties for noncompliance.

Answer: A

Explanation:

Adopting wearable technology requires ensuring that IT's infrastructure, processes, and standards can support the new initiative. The CGEIT Review Manual 8th Edition highlights that an enterprise architecture (EA) review is the best method to validate IT's preparedness, as it assesses the alignment of IT capabilities with the requirements of new technologies.

Extract from CGEIT Review Manual 8th Edition (Domain 4: Strategic Management):"To validate IT's preparedness for adopting new technologies, the CIO should request an enterprise architecture review. The EA review assesses whether current IT infrastructure, applications, and processes can support the technology initiative, identifying gaps and necessary adjustments." (Approximate reference: Domain 4, Section on Enterprise Architecture and Technology Adoption)

Requesting an enterprise architecture review (option A) ensures that the CIO evaluates IT's technical and operational readiness for wearable technology, including compatibility with existing systems, scalability, and security requirements.

Why not the other options?

B . Perform a baseline business value assessment: A value assessment focuses on benefits, not IT's technical preparedness, which is the primary concern here.

C . Request reprioritization of the IT portfolio: Portfolio reprioritization addresses resource allocation, not the technical readiness of IT systems.

D . Identify the penalties for noncompliance: Penalties are a risk management concern, not a direct method to validate IT preparedness.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 4: Strategic Management, Section on Enterprise Architecture and Technology Integration.

ISACA CGEIT Study Guide, Chapter on IT Readiness Assessment.

Question: 682

Which of the following is MOST helpful in determining whether an enterprise's quality assurance (QA) program is meeting business requirements?

A. Review the quality framework.
B. Perform a SWOT analysis.
C. Review service outage reports.
D. Perform a quality audit.

Answer: D

Explanation:

Determining whether a quality assurance (QA) program meets business requirements requires an objective evaluation of its effectiveness in delivering expected outcomes. The CGEIT Review Manual 8th Edition states that a quality audit is the most effective method to assess whether QA processes align with business needs, as it provides a structured review of performance and compliance.

Extract from CGEIT Review Manual 8th Edition (Domain 5: Benefits Realization):"A quality audit is the most effective way to determine whether an enterprise's quality assurance program meets business requirements. The audit evaluates the QA processes, controls, and outcomes against defined business objectives, identifying gaps and areas for improvement." (Approximate reference: Domain 5, Section on Quality Management and Assurance)

Performing a quality audit (option D) provides a comprehensive assessment of the QA program's alignment with business requirements, examining processes, metrics, and deliverables to ensure they meet stakeholder expectations.

Why not the other options?

A . Review the quality framework: Reviewing the framework provides insight into design but does not assess actual performance or alignment with business needs.

B . Perform a SWOT analysis: A SWOT analysis identifies strengths, weaknesses, opportunities, and threats but is too broad and not specific to evaluating QA effectiveness.

C . Review service outage reports: Outage reports may indicate issues but are limited to specific incidents and do not provide a holistic view of the QA program's alignment with business requirements.

Reference:

ISACA CGEIT Review Manual 8th Edition, Domain 5: Benefits Realization, Section on Quality Assurance and Auditing.

ISACA CGEIT Study Guide, Chapter on QA Program Evaluation.