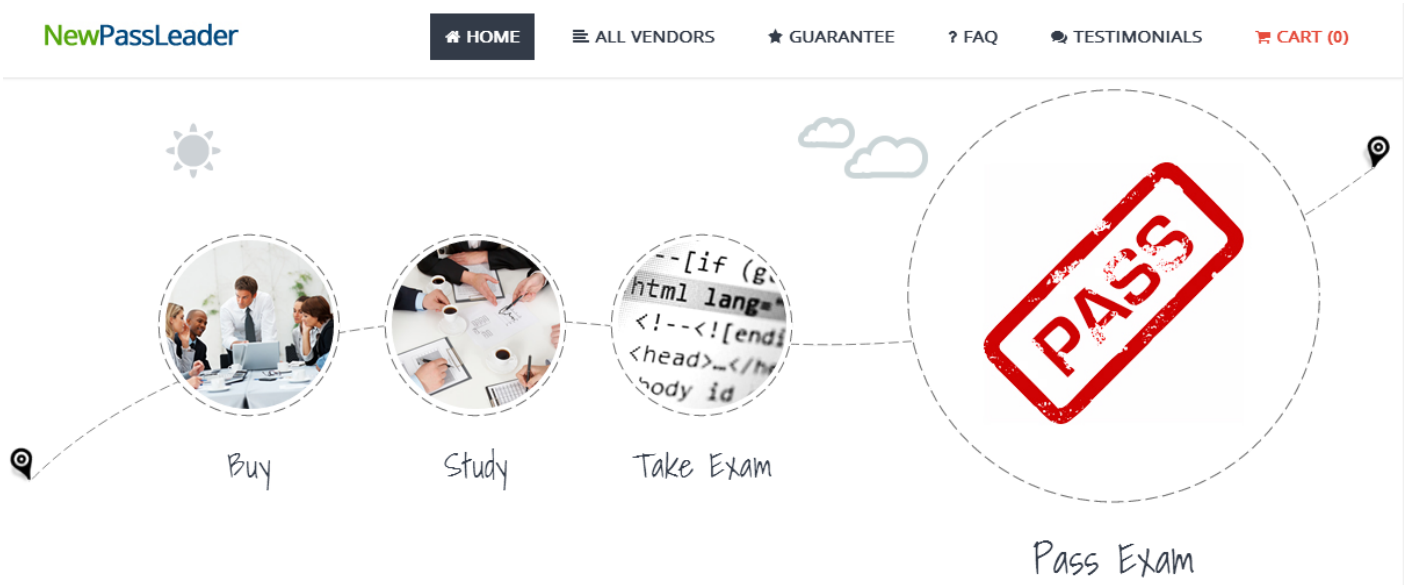
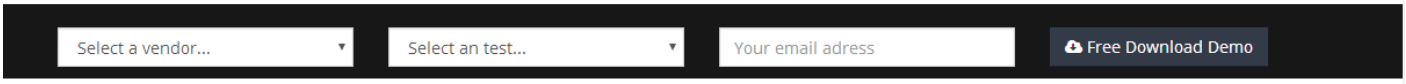
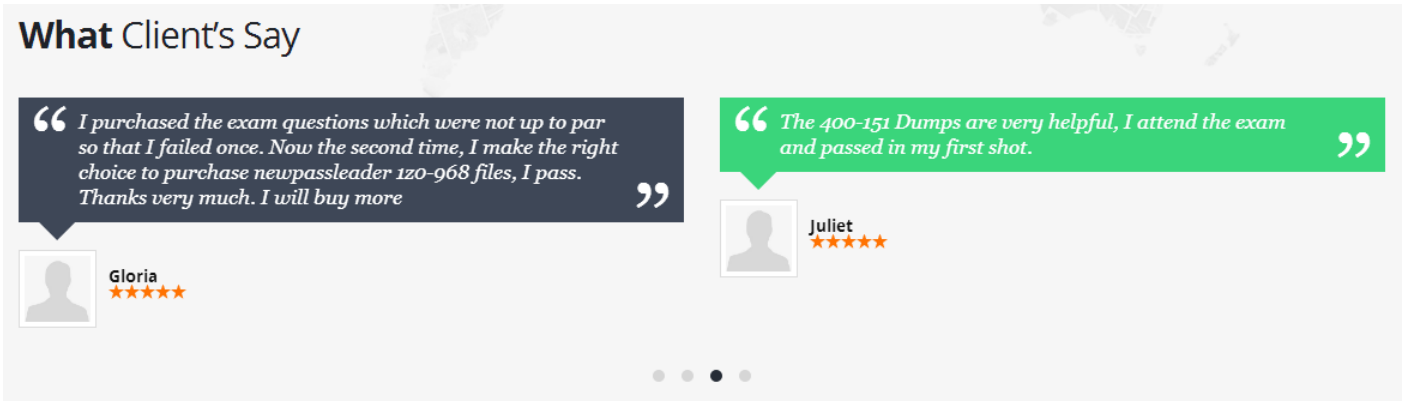
NewPassleader





Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
PDF format: Easy to read and print learning materials, our products are available in PDF file format.
Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



http://www.newpassleader.com/

Attentive Service Exam Torrent and Valid Dumps - NewPassLeader

Exam : **CGEIT**

Title : Certified in the Governance of Enterprise IT Exam

Vendor : ISACA

Version : DEMO

NO.1 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.

NO.2 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. References: ISACA, Performance Measurement Metrics for IT Governance, page 11. datapine, Top 20 IT KPIs - Explore The Best IT KPI Examples & IT Metrics

NO.3 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. References := Reducing Cybersecurity Security Risk From and to Third Parties; Unauthorized Access: Prevention Best Practices; Security of Enterprise Application Integration

NO.4 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.
References:
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.

NO.5 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.
References:
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.

NO.6 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. References := CGEIT Review Manual, 7th Edition, Chapter 1: Framework for the Governance of Enterprise IT, Section 1.4: GEIT Implementation Approaches, pp. 23-24.

NO.7 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." References := What is an IT Steering Committee? - BMC Software | Blogs

NO.8 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

NO.9 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. References: CGEIT Exam Candidate Guide, page
13. CGEIT Certification

NO.10 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.

NO.11 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 Explanation:

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.

NO.12 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. References: COBIT 2019, ISACA Security Guidance.

NO.13 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.
References:
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.

NO.14 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. References: : 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

NO.15 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 Explanation:

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 decision-making. 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.

NO.16 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. References:
COBIT 2019 Risk Management Process, CGEIT Exam Manual.

NO.17 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.
References:
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."

NO.18 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. References := 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.

NO.19 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.
References: 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 Self-Assessment - ISACA4 5:
Maturity Assessment - ISACA

NO.20 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 References:
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."

NO.21 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. References: 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.

NO.22 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. References: 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.

NO.23 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.

NO.24 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 long-term 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. References := What is Data Classification?, Data Governance Policy: Examples & Templates, What is data governance?

NO.25 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. References: CGEIT Exam Content Outline | ISACA1, CGEIT Review Manual (Digital Version), What is enterprise architecture? A framework for transformation | CIO2, Enterprise Architecture:
Definition, Benefits & Examples3

NO.26 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. References := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 23-24.

NO.27 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.

NO.28 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.

References := 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.

NO.29 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

NO.30 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).

NO.31 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.
References := 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.

NO.32 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

NO.33 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.
References: 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

NO.34 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.

NO.35 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 decision-making 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. References := ISACA, CGEIT Review Manual, 7th Edition, 2019, page 17.