ISACA CGEIT Exam Questions

Total Questions: 650+
Demo Questions: 35
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
ISACA CGEIT Exam Questions by Cert Empire

Question: 1

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 is the most effective tool for standardizing how sensitive corporate data is handled. This framework establishes categories for data based on its level of sensitivity, criticality, and value to the enterprise (e.g., Public, Internal, Confidential, Restricted). For each category, it defines specific, mandatory handling procedures for creation, storage, transmission, and destruction. This ensures that data is protected consistently and appropriately across the enterprise, directly fulfilling the objective of standardization. The framework provides the granular, actionable rules needed to implement the high-level goals of security and risk policies.

Why Incorrect Options are Wrong:

B. Enterprise risk policy: This is a high-level document that states the organization's overall intent and direction for managing risk; it does not provide specific, standardized data handling procedures.
C. Enterprise risk management (ERM) framework: An ERM framework provides a broad structure to identify and manage all types of enterprise risks, but it is not the specific tool for standardizing data handling rules.
D. Information security policy: While this policy mandates the protection of information, the classification framework is the specific component within it that operationalizes and standardizes how different types of data are handled.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020). Domain 4: Information Resources Optimization, Task Statement 4.02, states the need to "Ensure that information/data is classified in terms of criticality and sensitivity." The supporting text explains that this classification is essential to determine the required level of protection and appropriate handling procedures.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018).

Management Objective APO14, Managed Data, Practice APO14.02, "Define and implement a data classification scheme." The description states that this practice is necessary to "ensure that data is handled (e.g., stored, archived, destroyed, accessed) according to its classification." This directly links classification to standardized handling.
3. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018). Management Objective APO14, Managed Data, Practice APO14.03, "Manage the data life cycle." This practice explicitly requires enterprises to "Define and implement procedures for data handling, including labeling, handling, storage, retention, retrieval and secure disposal, according to classification."

Question: 2

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:

The most critical consideration is ensuring the vendor's business continuity plan (BCP) aligns with the enterprise's own BCP requirements for the critical application. This alignment, particularly concerning Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), is fundamental. If a vendor's plan, however well-tested or audited, cannot meet the recovery timeline the business requires, the vendor is not a viable partner for a critical service. Strategic alignment must be established before other due diligence activities, such as testing or reviewing audit reports, can provide meaningful assurance. This is a core principle of IT governance: ensuring third-party services support enterprise objectives.

Why Incorrect Options are Wrong:

A. Procuring a copy of the vendor's BCP is a necessary preliminary step, but simply possessing the document does not confirm its adequacy or alignment with enterprise needs.
B. Testing the vendor's BCP is an excellent assurance activity, but it is secondary to ensuring the plan's objectives align with the enterprise's requirements in the first place.
C. Obtaining independent audit reports provides third-party assurance, but these reports validate the vendor's controls against a standard, not necessarily against the enterprise's specific RTO/RPO needs.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020). Domain 4: Risk Optimization, Section 4.4, "Business Continuity and Disaster Recovery." This section emphasizes that IT continuity plans, including those of third-party providers, must be integrated with and support the enterprise's overall business continuity plan and its requirements. The alignment of objectives is paramount.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018). Management Objective DSS04, "Managed Continuity," Practice DSS04.02, states the need to

"Define a business continuity policy, objectives and scope... based on business requirements." When a vendor provides a critical service, their continuity objectives must align with these business-driven requirements.

3. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018). Management Objective APO10, "Managed Vendors," Practice APO10.04, discusses the need to "Select vendors based on their ability to meet requirements." For a critical application, business continuity capabilities are a key requirement that must be evaluated for alignment.

Question: 3

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:

The core issue is a strategic misalignment between the organization's new strategy and its IT human resource capabilities, specifically regarding retention. IT governance is responsible for ensuring that IT resources, including personnel, are optimized to support enterprise goals. Directing the development of a strategic HR plan for IT is the most comprehensive and appropriate governance-level response. This plan would holistically address recruitment, training, career development, succession planning, and compensation, ensuring a long-term, sustainable solution that is directly aligned with the new business strategy. The other options are tactical and address only single facets of the larger retention problem.

Why Incorrect Options are Wrong:

A. Implement an incentive-based employee referral program: This is a tactical recruitment tool, not a comprehensive retention strategy. It fails to address the root causes of why existing qualified personnel are leaving.
C. Recommend enhancements to the online recruiting platform specific to IT: This is a specific, operational tactic focused on attracting new talent. It does not address the stated problem of retaining current, qualified staff.
D. Work with HR to enhance compensation packages for IT personnel: While important, compensation is only one component of employee retention. This is a tactical response, whereas a strategic plan would provide a more complete and effective solution.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020). Domain 3: Resource Optimization, Task 3.2, states the need to "Ensure that IT has sufficient, competent, and motivated human resources." This involves establishing processes for acquiring, training, and retaining personnel. A strategic HR plan is the formal mechanism to structure and direct these processes, making it a

primary governance concern.

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018). The management objective APO07 Managed Human Resources has the purpose to "Optimize human resource capabilities to meet enterprise objectives." Key management practices like APO07.03 ("Maintain the skills and competencies of personnel") and APO07.01 ("Maintain adequate and appropriate staffing") are best managed through a cohesive strategic plan. The governance body's role is to direct and monitor that such a plan is in place and effective.

3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 3, "IT Governance Mechanisms," discusses the role of structures and processes. A strategic HR plan for IT is a critical process mechanism that a governance body would ensure is established to align human resources with strategic objectives. It is a directive action, distinct from the specific implementation tactics in the other options. (DOI: 10.1007/978-3-319-14547-1)

Question: 4

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:

Enterprise architecture (EA) is the most effective approach for planning IT-enabled investments because it provides a holistic, strategic blueprint of the enterprise. EA aligns business strategy with IT strategy by defining the current and desired future states of business processes, data, applications, and technology infrastructure. This framework allows stakeholders to make informed investment decisions, ensuring that new initiatives support long-term objectives, integrate with existing capabilities, avoid redundancy, and deliver maximum business value. It serves as a roadmap for change, making it the foundational tool for strategic investment planning.

Why Incorrect Options are Wrong:

B. IT process mapping is a tactical tool used to document and analyze specific workflows; it lacks the strategic, enterprise-wide perspective required for investment planning.
C. Task management is an operational activity focused on organizing and tracking individual work items, which is far too granular for strategic investment decisions.
D. Service level management is concerned with monitoring and managing the performance of IT services after they are implemented, not with the initial planning of investments.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 2: IT Resources, Task Statement 2.1, "Evaluate, direct and monitor IT resource planning, use and allocation...". The associated knowledge statement K2.1.1, "Knowledge of enterprise architecture (EA) principles and frameworks," directly links EA to the strategic planning of IT resources and investments.
2. Ross, J. W., Weill, P., & Robertson, D. C. (2006). Enterprise Architecture as Strategy: Creating a Foundation for Business Execution. Harvard Business School Press. Chapter 1, "Foundations of Execution," explains how EA provides the organizing logic for business processes and IT infrastructure, which is essential for guiding IT investment decisions to support strategic goals.
3. Tamm, T., Seddon, P. B., Shanks, G., & Reynolds, P. (2011). How does enterprise architecture

add value to organisations? Communications of the Association for Information Systems, 28(1), Article 10. This paper discusses how EA contributes to organizational benefits, including improved IT investment decision-making by providing a long-term perspective that aligns IT with business needs (pp. 146-148).

Question: 5

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:

Key Risk Indicators (KRIs) are metrics used to provide an early warning of increasing risk exposure in a specific area. They are fundamentally tied to the potential for an adverse event to impact the achievement of objectives. Therefore, the IT goals and objectives must be defined first. Without a clear understanding of what the enterprise is trying to achieve through IT, it is impossible to identify the relevant risks that could impede success or to establish meaningful indicators to monitor those risks. The entire risk management process, including the definition of KRIs, is driven by and aligned with the strategic objectives of the organization.

Why Incorrect Options are Wrong:

A. IT resource strategy: This strategy is developed to support the achievement of defined IT goals; it is a means to an end, not the starting point for risk identification.
B. IT risk and security framework: The framework provides the structure and process for managing risk, but the specific risks and KRIs are derived from the goals the framework is designed to protect.
D. IT key performance indicators (KPIs): Both KPIs and KRIs are derived from goals and objectives. KPIs measure performance toward goals, while KRIs measure risk exposure related to achieving those same goals.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 3: Risk Optimization, Section 3.4, p. 129. The manual states, "KRIs are metrics that provide an early warning of a potential risk event... They should be linked to specific business objectives to be effective." This confirms that objectives must be defined first.
2. ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. Chapter 4: The COBIT Goals Cascade, p. 31. This core COBIT concept illustrates that stakeholder needs and enterprise goals are the primary drivers for all governance and management objectives, which include risk management activities.

3. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Process APO12 Manage Risk, p. 103. The purpose statement for this process is to "Integrate the management of IT-related enterprise risk with overall enterprise risk management (ERM) and to balance the costs and benefits of managing IT-related enterprise risk." This integration is predicated on alignment with enterprise objectives.

Question: 6

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 fundamental principle of the Governance of Enterprise IT (GEIT) is to create value by meeting stakeholder needs. The IT strategy must be directly aligned with the enterprise's overall strategy and objectives, which are defined and driven by key stakeholders (e.g., the board, executive management, business leaders). Therefore, consulting with these stakeholders is the CIO's greatest consideration when making changes. This ensures the revised IT strategy remains aligned with business needs, has the necessary support and buy-in, and is positioned to deliver the expected value to the enterprise.

Why Incorrect Options are Wrong:

A. Assessing the impact on the enterprise architecture (EA) is a critical step for implementation, but it follows the strategic decision, which must first be aligned with stakeholder needs.
B. Revising the investment portfolio is a direct consequence of a strategic change used to fund the new direction, not the primary consideration for making the change itself.
D. Adjusting IT risk metrics is a necessary risk management activity to align with the new strategy, but it is a supporting function, not the primary driver for the strategic change.

References:

1. ISACA, CGEIT Review Manual, 8th Edition, 2020. In Domain 2: Strategic Management, Section 2.2.1, "Enterprise and IT Strategy Alignment," it is stated, "The first step in developing an IT strategy is to understand the enterprise strategy... This understanding is gained through communication with key stakeholders, including the board of directors, executive management and business process owners." This establishes stakeholder consultation as the foundational step.
2. ISACA, COBIT 2019 Framework: Introduction and Methodology, 2018. The first component of the governance system is "Processes." The governance objective EDM02 Ensured Benefits

Delivery emphasizes optimizing value through a portfolio of IT-enabled investments, which is directly linked to understanding and satisfying stakeholder needs and strategic objectives (p. 39).
3. ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2018. The description for process APO02 Manage Strategy states its purpose is to "Align IT and enterprise strategies, by understanding the enterprise strategy and environment... and proposing ways for IT to create and deliver value." This process inherently involves deep engagement with enterprise stakeholders (p. 51).

Question: 7

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 most critical information to provide to an independent consultant before an audit begins is the audit's scope and stakeholders. The scope defines the precise boundaries of the engagement-what systems, processes, and time periods are to be examined. The stakeholders identify who the audit is for and who needs to be involved. This information is foundational for creating the audit charter or terms of reference, which authorizes the audit and sets clear expectations. Without a defined scope, the consultant cannot effectively plan the audit, allocate resources, or ensure the final report addresses the specific concerns of the IT governance committee and the board.

Why Incorrect Options are Wrong:

A. Acceptance of the audit risks and opportunities: This is part of the audit planning process, but it can only be determined after the scope is defined and an initial risk assessment is performed.
C. The organizational structure of the security office: This is important evidence that will be reviewed during the audit to understand roles and responsibilities, but it is not a prerequisite for defining the audit's purpose and boundaries.
D. The policies and framework used by the security office: These are key documents to be assessed for compliance and effectiveness within the defined scope of the audit, not before the scope itself is established.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 4, Task Statement T4.3, emphasizes providing assurance that risk management practices are effective. To provide this assurance, any audit or review must have a clearly defined scope and objective to guide the work. The scope is the primary determinant of the audit's direction.
2. ISACA, ITAFTM: A Professional Practices Framework for IT Assurance, 4th Edition. Standard

S7, "Audit Charter," states, "The purpose, responsibility, authority and accountability of the IT audit function or IT audit activities should be documented in an audit charter." For an ad hoc engagement, the terms of reference or engagement letter serves this purpose, and its primary components are the scope and objectives.
3. ISACA, ITAFTM: A Professional Practices Framework for IT Assurance, 4th Edition. Guideline G13, "Use of an External Service Provider," notes the importance of a formal agreement that "should clearly state the scope of the work to be performed." This is paramount when engaging an external party like an independent consultant.

Question: 8

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:

The success of an IT governance implementation plan is critically dependent on its adoption and integration within the enterprise. Organizational culture, which encompasses the shared values, beliefs, and behaviors, is the most significant factor influencing how change is accepted and managed. A plan designed without considering the existing culture is likely to encounter resistance, leading to low adoption rates and ultimate failure. Therefore, tailoring the implementation approach, communication strategy, and change management activities to the specific cultural context is the most important consideration for ensuring the plan is realistic, effective, and sustainable.

Why Incorrect Options are Wrong:

A. Principles and policies are the core components of the governance framework; they are what is being implemented, not the primary consideration for the implementation plan's design.
B. Roles and responsibilities are essential elements defined within the governance framework, but their successful assignment and execution depend heavily on the organization's cultural acceptance.
C. Risk tolerance levels are a key strategic input that helps define the content and objectives of the governance framework, rather than the methodology for its implementation.

References:

1. ISACA, CGEIT Review Manual, 8th Edition, 2020. In Domain 4: Governance Implementation, Task G4.1, the manual emphasizes that the implementation plan must be tailored to the specific context of the enterprise, which explicitly includes its culture, to ensure success.
2. ISACA, COBIT 2019 Implementation Guide, 2018. Chapter 4, "The Implementation Life Cycle," details the phases of implementation. Phase 3, "Create a desire to change," and Phase 5, "Embed new approaches," are entirely focused on managing organizational and behavioral change, underscoring that cultural readiness is a prerequisite for successful implementation.

3. De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. Information Systems Management, 26(2), 123-137. The study highlights that implementing IT governance is fundamentally an organizational change initiative, and factors like communication and resistance to change (cultural elements) are critical success factors. (https://doi.org/10.1080/10580530902794786)

Question: 9

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 fundamental principle of enterprise governance, as emphasized in the CGEIT framework, is that it is driven by stakeholder needs and the creation of value. When addressing a complex and sensitive issue such as potential discrimination from machine learning (ML), the FIRST and most critical step is to understand the ethical boundaries and expectations of all relevant stakeholders. This includes customers, employees, regulators, and the community. Obtaining this input establishes the foundational ethical principles and risk appetite upon which all subsequent governance actions, such as policy development (C), code of conduct revisions (B), and legal assessments (D), will be based.

Why Incorrect Options are Wrong:

B. Revise the code of conduct to discourage bias within automated processes: Revising a code of conduct is a necessary action, but it must be guided by pre-established ethical principles, which are determined through stakeholder engagement.
C. Develop a machine learning policy articulating guidelines for machine learning use: A policy is a formalization of the enterprise's stance and rules. This stance must first be defined by understanding stakeholder concerns and ethical requirements.
D. Assess recent case law related to the enterprise's machine learning business strategy: While essential for compliance, a legal assessment addresses only the legal risks. Ethical concerns often extend beyond current law, and stakeholder expectations are the primary driver for governance.

References:

1. ISACA, CGEIT Review Manual, 7th Edition. Domain 1, Section 1.4, "Governance Framework Principles." The manual emphasizes that a primary objective of governance is to create value for stakeholders. This principle necessitates that the initial step in any governance initiative is to identify and understand stakeholder needs and expectations to guide the framework's direction.
2. ISACA, COBIT 2019 Framework: Introduction and Methodology. Chapter 3, "The COBIT Core Model," Figure 3.1, "COBIT Core Model." This figure illustrates the goals cascade, which explicitly begins with "Stakeholder Drivers and Needs." This foundational concept dictates that all governance and management objectives are derived from stakeholder requirements.
3. ISACA, "AI Ethics: A New Frontier for Governance," White Paper, 2021. Page 6, "Establishing an AI Ethics Framework." The paper states, "The first step in establishing an AI ethics framework is to define the organization's ethical principles for AI. This process should involve a diverse group of stakeholders..." This directly supports obtaining stakeholder input as the initial action.
4. ISACA, COBIT 2019 Framework: Governance and Management Objectives. EDM03, "Ensured Risk Optimization." The description for this governance objective includes key activities such as understanding the enterprise's risk appetite and tolerance, which are defined in consultation with key stakeholders. Addressing discrimination is a form of risk optimization.

Question: 10

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 risk analysis is the most appropriate method for assessing risk scenarios where potential "economic loss" is the primary concern. This methodology uses numerical values, primarily monetary, to determine the potential financial impact of a risk. It calculates metrics such as Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE), providing a concrete financial figure for the identified risks. This allows the enterprise to prioritize risks based on their financial severity and make informed, data-driven decisions about risk response and the allocation of resources for mitigation, which is essential for major IT investments.

Why Incorrect Options are Wrong:

A. Cost-benefit analysis: This is a project justification tool used to compare the financial benefits of an investment against its costs, not a method for assessing the risk of potential loss.
B. Qualitative analysis: This method uses subjective, descriptive scales (e.g., high, medium, low) and is less precise for scenarios where a specific economic or monetary value of loss needs to be assessed.
C. Business impact analysis (BIA): This analysis focuses on identifying the operational and financial impacts of a disruption to critical business processes, primarily to inform business continuity and disaster recovery planning.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 3: Risk Optimization, Section 3.2, Task T3.2, Knowledge Statement K3.2.2. The manual distinguishes between quantitative analysis, which assigns monetary values to risk components, and qualitative analysis, which uses descriptive ratings. It positions quantitative analysis as the method for determining financial impact.
2. ISACA. (2020). The Risk IT Framework, 2nd Edition. Process RE 2: Analyze Risk. This

framework details that quantitative risk analysis "is preferred to support the cost-benefit analysis of risk responses" because it expresses risk in numerical terms, such as monetary value, which directly addresses the assessment of economic loss.

3. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. APO12 Manage Risk, APO12.03 Analyze risk. This practice involves identifying the potential business impact of risk, which, when expressed in financial terms, necessitates a quantitative approach to provide a clear basis for evaluation.

Question: 11

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 purpose of an information classification scheme is to ensure that information assets are protected in a manner commensurate with their value to the organization. This value is determined by assessing the potential adverse business impact-such as financial loss, reputational damage, regulatory penalties, or operational disruption-that could result from the unauthorized disclosure, modification, or unavailability of the information. Therefore, business impact analysis is the foundational activity that drives the definition of classification categories (e.g., Public, Confidential, Restricted) and their corresponding security controls.

Why Incorrect Options are Wrong:

A. Information architecture defines how information is structured and organized; it is a consumer of the classification scheme, not the basis for creating it.
B. Industry standards provide valuable frameworks and best practices for creating a classification scheme, but the specific categories must be based on the organization's unique risk and impact profile.
C. Information security policy is the formal document that mandates and communicates the classification scheme; the scheme itself is based on business impact, which then informs the policy.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020): Domain 2: IT Resources Optimization, Section 2.4, discusses that information classification is based on its criticality and sensitivity to the organization. Criticality is a direct measure of business impact.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018): The management objective APO14, Managed Data, specifically practice APO14.02, emphasizes the need to "Classify data in accordance with the data classification policy according to its criticality to the business."

3. ISACA, "Data Classification: A Prerequisite for Effective Information Protection and Governance" (2021): This white paper states, "The first step in data classification is to define the criteria for each classification level. These criteria should be based on the potential impact to the organization if the data is compromised." (Page 4).

Question: 12

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:

An enterprise architecture (EA) review is the most comprehensive method for a CIO to validate IT's preparedness for a significant new technology initiative like wearables. EA provides a holistic blueprint of the enterprise's current business processes, data, applications, and technology infrastructure. By conducting an EA review, the CIO can assess the impact of the new technology across all these domains, identify necessary changes, evaluate integration challenges, and ensure the existing or planned architecture can support the initiative's strategic goals. This structured assessment directly addresses the question of IT's readiness to adopt and support the new technology effectively.

Why Incorrect Options are Wrong:

B. Request reprioritization of the IT portfolio is an action taken to allocate resources once an initiative is approved; it does not validate the technical or architectural readiness to undertake it.
C. Performing a baseline business value assessment is crucial for justifying the initiative and measuring its success later, but it evaluates business outcomes, not IT's technical preparedness.
D. Identifying penalties for noncompliance is a specific risk management activity. While important, it is too narrow and does not provide a comprehensive view of IT's overall readiness.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 2: IT Resources, Task 2.2 states the need to "Ensure that the enterprise architecture (EA) supports the achievement of enterprise goals and objectives." An EA review is the mechanism to validate this support for a new initiative.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The management objective APO03 Manage Enterprise Architecture is designed to "enable a standard, responsive and efficient delivery of operational and strategic objectives." A review of the EA is the primary way to assess the impact and readiness for new technologies against this standard.
3. Ross, J. W., Weill, P., & Robertson, D. C. (2006). Enterprise Architecture as Strategy: Creating

a Foundation for Business Execution. Harvard Business Review Press. Chapter 1, "Foundations for Execution," explains that EA provides the organizing logic for business processes and IT infrastructure, making it the essential tool for assessing readiness for strategic change.

Question: 13

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:

The primary function of an IT strategy committee is to provide strategic-level guidance and ensure that IT strategy is aligned with the overall enterprise strategy. This committee typically consists of board members and senior executives. Its key responsibility is to advise the board of directors on IT-related strategic matters, including the development of IT goals, principles, and policies that will enable the achievement of business objectives. This advisory role ensures that IT is considered a strategic enabler from the highest level of the organization.

Why Incorrect Options are Wrong:

A. Providing oversight on enterprise strategy implementation is the responsibility of the board of directors and executive management, not a subcommittee focused specifically on IT.
B. The board of directors is responsible for approving the overall business strategy. The IT strategy committee focuses on the IT components that support that approved strategy.
D. Tracking projects in the IT investment portfolio is a more tactical, management-level function, typically handled by an IT steering committee or a program/project management office (PMO).

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020): Domain 1: Governance of Enterprise IT, Section 1.5.2, Organizational Structures, Roles and Responsibilities. This section describes the IT strategy committee's role as providing advice and direction to the board on IT strategy, ensuring alignment with enterprise goals. It distinguishes this strategic function from the more tactical oversight of an IT steering committee.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018): Governance Objective EDM01 (Ensured Governance Framework Setting and Maintenance) and Management Objective APO02 (Managed Strategy). These objectives detail the organizational structures required for effective governance. The framework outlines the need for a structure, such as an IT strategy committee, to advise the governing body (the board) on IT-related strategy to ensure value creation. (See EDM01.02, "Direct the establishment of organizational structures,"

and related RACI charts).
3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 3, "Implementing IT Governance Structures, Processes, and Relational Mechanisms," discusses the roles of different committees. It specifies that the IT Strategy Committee operates at the board level to assist the board in its IT-related responsibilities, primarily by providing strategic advice. (DOI: 10.1007/978-3-319-14547-1).

Question: 14

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 foundational step in establishing any risk management process is to identify and inventory the assets that are critical to the organization's objectives. Assets include information, technology infrastructure, processes, and people. Without a comprehensive understanding of what the organization values and needs to protect, it is impossible to effectively identify relevant threats, analyze vulnerabilities, or assess the potential impact of a risk event. Asset identification provides the essential context for all subsequent risk management activities, ensuring that resources and controls are appropriately focused on protecting what is most important to the enterprise.

Why Incorrect Options are Wrong:

A. Determining the probability of occurrence is a component of risk analysis, which can only be performed after an asset and its associated threats have been identified.
B. Threats are identified in relation to the assets they could potentially harm. Therefore, identifying the assets must precede the identification of threats against them.
D. Assessing risk exposures is a comprehensive evaluation step that synthesizes information about assets, threats, and vulnerabilities; it is not the starting point of the process.

References:

1. ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2018. The management objective APO12 Manage Risk includes practice APO12.02 Collect data. The description for this practice states, "Identify and collect relevant data to enable effective IT-related risk identification, analysis and reporting. This includes identifying key stakeholders and the assets at risk." This places asset identification at the very beginning of the risk identification and analysis phase. (APO12.02, page 121).
2. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012. This foundational guide, widely referenced in IT governance, outlines the risk assessment process. The first step described in the assessment process itself is System Characterization. The guide states, "The

first step in any risk assessment is to characterize the systems and the information processed, stored, and transmitted by those systems... This includes identifying... system assets (e.g., hardware, software, firmware, etc.)." (Section 2.2.1, Page 23).
3. ISACA, CGEIT Review Manual, 8th Edition, 2020. In Domain 3, Risk Optimization, the process of risk identification is detailed. It emphasizes that risk identification begins with understanding the business context, which involves identifying the critical IT processes and the assets that support them. This establishes the scope and foundation before threats or probabilities can be considered. (Domain 3, Section 2: Risk Identification).

Question: 15

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:

Implementing knowledge management practices is the most strategic and sustainable long-term solution. It involves systematically capturing, documenting, sharing, and managing the critical knowledge and experience held by staff. This transforms individual expertise into an organizational asset, ensuring that valuable information is retained and accessible even after experienced employees depart. This approach directly mitigates the risk of knowledge loss, supports continuity, and facilitates the training of new staff, making it the most comprehensive and enduring solution among the choices.

Why Incorrect Options are Wrong:

B. A mentoring program is a useful tactic for knowledge transfer but is often informal and dependent on the individuals involved, making it less systematic than a full knowledge management program.
C. Determining key risk indicators (KRIs) is a diagnostic activity. It helps in identifying and monitoring the risk of staff loss but does not constitute a solution to address the actual loss of knowledge.
D. Retaining key staff as consultants is a reactive, short-term measure. It can be costly and creates a continued dependency on individuals outside the organization, rather than building internal capability.

References:

1. ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Management Objective BAI08 - Managed Knowledge. The objective's description states its purpose is to "Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making." This directly supports creating a system to retain knowledge independent of specific individuals.
2. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 3: Resource Optimization, Section

3.4, Task T3.4. This section emphasizes the need to "Ensure the availability of sufficient and capable IT resources to support enterprise objectives," which includes managing human capital and the knowledge they possess through structured means like knowledge management systems to ensure business continuity.
3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 4, "Enablers for the Governance of Enterprise IT," discusses the importance of the "People, Skills and Competencies" enabler, highlighting that processes must be in place to manage and retain knowledge to mitigate risks associated with staff turnover and ensure long-term capability. (DOI: 10.1007/978-3-319-14547-1)

Question: 16

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:

A Business Impact Analysis (BIA) is a foundational step in the business continuity management (BCM) lifecycle. It identifies critical business processes and quantifies the potential operational and financial impacts of their disruption. Once the enterprise understands which processes are most critical and the impact of their failure, the logical next step is to evaluate and select appropriate strategies to mitigate these risks and ensure recovery. This involves assessing various options (e.g., alternate sites, redundant systems, manual workarounds) to determine the most cost-effective approach to meet the recovery objectives defined in the BIA. This strategy selection phase precedes the development or updating of detailed plans.

Why Incorrect Options are Wrong:

A. A risk controls gap analysis is performed after mitigation strategies are chosen to determine if existing controls are sufficient to implement the selected strategy.
B. Updating the disaster recovery plan (DRP) is a subsequent, tactical step that implements the chosen recovery strategies; the high-level strategy must be assessed and selected first.
C. Verifying compliance is an ongoing governance activity and a key input/driver for the BIA, not the immediate sequential step following its completion.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 4: Risk Optimization, Section 4.2, Task Statement T4.2: "Manage IT risk to an acceptable level to meet business requirements." The BIA is a key input to this process, which inherently involves assessing mitigation options to manage the identified risks. The process flows from impact analysis (BIA) to risk assessment and then to selecting treatment/mitigation strategies.
2. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 2: IT Resources, Section 2.5, Knowledge Statement K2.5.2: "Business continuity plan (BCP) and disaster recovery plan (DRP) development and testing methods." The development of these plans is predicated on a strategy

derived from the BIA and risk assessment. The manual describes the BCM lifecycle where strategy definition follows the BIA.

3. Whitman, M. E., & Mattord, H. J. (2019). Management of Information Security (6th ed.). Cengage Learning. Chapter 5, "Risk Management: Identifying and Assessing Risk," outlines the standard risk management framework where a BIA is conducted to determine mission/business process priorities, which is then followed by the evaluation of risk mitigation strategies before developing specific contingency plans. This sequence is standard academic and professional practice.

Question: 17

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:

Following a major acquisition and the introduction of a new business strategy, the foundational step for the CIO is to conduct a gap analysis. This involves a thorough review of the existing IT strategy against the new enterprise strategy. This assessment is critical to understand the current state, identify misalignments, and determine what elements of the IT strategy are still relevant, what must be changed, and what new capabilities are required. This review provides the essential, evidence-based foundation upon which all subsequent actions, such as revising the strategy or restructuring governance, will be built. Acting without this initial analysis would be premature and risk creating an IT strategy that is not fully aligned with the new business direction.

Why Incorrect Options are Wrong:

B. revise the existing IT strategy to align with the new business strategy: Revision is a necessary subsequent step, but it cannot be performed effectively without first completing the review and gap analysis described in option A.
C. establish a new IT strategy committee for the new enterprise: While governance structures are vital, creating a new committee is a structural change that should be informed by the revised strategy, not precede the strategic review itself.
D. assess the IT cultural aspects of the acquired entity: Cultural assessment is important for successful integration and execution, but the primary step for strategic alignment is to first align the formal strategies and plans.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020): Domain 1, Section 1.3, "Strategic Management," emphasizes that the IT strategic planning process begins with a deep understanding of the enterprise's direction. The manual states, "The first step in the IT strategic planning process is to gain a deep understanding of the enterprise and its direction... This

understanding is then used to create an IT strategy that is fully aligned with and supports the enterprise." (p. 41). This supports reviewing the new business strategy first.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018): The management objective APO02 Manage Strategy outlines a clear process. Practice APO02.01 is to "Understand enterprise context and direction." Practice APO02.02 is to "Assess the current environment, capabilities and performance." These two initial practices are encapsulated in the act of reviewing the existing IT strategy against the new business strategy before moving to subsequent practices like "Conduct a gap analysis" (APO02.04) and "Define the strategic plan and road map" (APO02.05).

Question: 18

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 primary role of a governance body, such as an IT strategy committee, is to provide direction and ensure alignment between IT and enterprise objectives. After establishing stakeholder desired outcomes (which define the enterprise's goals and risk appetite), the most critical and logical next step is to ensure the IT risk management program is aligned with the overall enterprise risk management (ERM) framework. This strategic alignment ensures that IT risk is managed in the context of business objectives and priorities, providing the foundational direction for all subsequent tactical risk management activities.

Why Incorrect Options are Wrong:

A. identify business data that requires protection.
This is a specific, tactical task within the risk identification phase of risk management, not the main strategic goal of a governance committee.
B. perform a risk analysis on key IT processes.
This is an operational activity within the risk management process. The committee's role is to oversee and direct, not to perform the analysis itself.
C. implement controls to address high risk areas.
This is a risk treatment/response activity that occurs after risk has been identified and analyzed. It is a tactical implementation, not the initial strategic goal.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 4: Risk Optimization, Section 4.2, "IT Risk Strategy in Support of Business Strategy." This section explicitly states that the IT risk strategy must be aligned with the enterprise risk strategy to ensure that IT risk management activities are consistent with the enterprise's overall risk appetite and tolerance. This alignment is a fundamental governance responsibility.

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. Governance Objective EDM03, "Ensure Risk Optimization." The description for this objective emphasizes ensuring that IT-related enterprise risk is managed in line with the enterprise's governance objectives and risk appetite. Practice EDM03.01, "Evaluate risk management," involves directing the establishment of an IT risk management approach that is aligned with the enterprise risk management (ERM) approach.
3. ISACA, The Risk IT Framework, 2nd Edition. Part II, Section 2.1, "Risk Governance." This section highlights that a key objective of IT risk governance is to "Establish and maintain a common risk view" and "Integrate IT risk management with enterprise risk management (ERM)." This integration ensures that IT risk is considered alongside other enterprise risks, which is the essence of alignment.

Question: 19

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 most critical first step upon learning of a new regulation is to understand its potential impact. A risk assessment accomplishes this by analyzing the regulation's requirements, identifying potential gaps in current processes, and evaluating the consequences of non-compliance. This assessment provides the necessary factual basis for all subsequent activities, including informing the board, developing action plans, and determining if the existing risk management framework is adequate. Acting without this initial analysis would be based on assumptions rather than a clear understanding of the risk, leading to ineffective or inappropriate responses.

Why Incorrect Options are Wrong:

A. Update the risk management framework: This is premature. The existing framework should guide the risk assessment. An update should only be considered if the assessment reveals a fundamental gap in the framework's ability to manage this type of risk.
B. Determine whether the board wants to comply with the regulation: The board requires the results of a risk assessment to make an informed decision. Presenting the issue without a clear understanding of the impact, costs, and risks is not effective governance.
D. Request an action plan from the risk team: An action plan is a response to an identified and understood risk. The risk must first be assessed to determine the necessary actions. Creating a plan without a prior assessment is illogical.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 3: Risk Optimization, Task Statement R1.2, states the need to "Analyze and evaluate risk to determine the enterprise's risk profile in order to provide IT risk information to stakeholders." This analysis (assessment) is a foundational step that precedes risk response (action planning) or high-level strategic decisions.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The process for APO12 Manage Risk outlines a clear sequence. APO12.02 Analyze risk is described as the step

to "Develop a comprehensive view of the potential business impact of IT risk...". This analysis must occur before subsequent steps like APO12.04 Articulate risk (informing the board) and APO12.05 Define a risk management action portfolio (creating an action plan).

3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 4, "IT-Related Risk and Resource Management," emphasizes that the risk management process begins with risk identification and analysis (assessment). The outputs of this phase are essential inputs for risk evaluation and response, which involve decision-making by senior management and the creation of mitigation plans. (DOI: 10.1007/978-3-319-14547-1).

Question: 20

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 balanced scorecard (BSC) is a strategic performance management framework designed to translate an organization's strategy into a set of measurable objectives and key performance indicators (KPIs). An IT BSC is cascaded from the enterprise-level scorecard, creating a direct and traceable link between IT objectives and business goals across multiple perspectives (e.g., financial, customer, internal process, learning and growth). This provides a holistic and comprehensive view, making it the most effective tool for a CIO to continuously monitor and report on the alignment between IT activities and the overall business strategy.

Why Incorrect Options are Wrong:

A. Key risk indicators (KRIs) are metrics focused on risk exposure. While important, they only represent the risk aspect of strategy, not the full picture of strategic alignment.
B. IT services supporting business processes is an operational-level review. It confirms IT is delivering services but does not provide a strategic view of alignment with business objectives.
D. The risk register is a repository for identified risks. It is a tool for risk management, not a comprehensive framework for monitoring overall strategic performance and alignment.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 1: Governance of Enterprise IT, Section 1.10 Performance Monitoring. The manual explicitly describes the balanced scorecard as a key tool for translating strategy into action and measuring IT's contribution to the business, thus monitoring alignment.
2. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Process EDM02 Ensured Benefits Delivery. This process emphasizes the need to monitor value optimization, which is achieved by cascading enterprise goals to IT-related goals and measuring them, a core principle of the BSC methodology.
3. Van Grembergen, W., & De Haes, S. (2009). Enterprise Governance of Information

Technology: Achieving Strategic Alignment and Value. Springer. Chapter 4, "The IT Balanced Scorecard," details how the BSC is a primary mechanism for implementing, measuring, and managing the IT strategy and its alignment with business strategy.

Question: 21

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 foundational step in aligning resource management with the IT strategic plan is to understand the disparity between the current resource capabilities and the future resource requirements dictated by that plan. This process is known as a gap analysis. It systematically identifies shortfalls or surpluses in skills, infrastructure, and applications needed to achieve strategic objectives. The output of this analysis provides the essential data to formulate a resource plan, which will then guide subsequent actions such as assigning roles, defining responsibilities, and evaluating sourcing strategies. Without first identifying the "gap," any resource management activities would lack strategic direction.

Why Incorrect Options are Wrong:

A. A RACI chart is a detailed implementation tool used to clarify roles, which is premature before the required resources and tasks are identified through a gap analysis.
B. Assigning roles and responsibilities is a component of executing a resource plan, which can only be developed after understanding the resource gaps.
D. Identifying outsourcing opportunities is a potential strategy to address a resource gap; the gap must be identified first before solutions can be considered.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 2: IT Resources Optimization, Section 2.2, IT Resource Planning. The manual states that after understanding the strategic direction, "A gap analysis can then be performed to identify the differences between the current and desired future states. This analysis helps in creating a roadmap for acquiring, developing, and managing the necessary IT resources."
2. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. APO07 Managed Human Resources. The process description for APO07.01 includes "Identify the skills and competencies required to meet the enterprise's objectives." This implies a comparison (gap analysis) between required and existing skills as a primary step.

3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 3, "IT Governance Mechanisms," discusses strategic alignment, noting that a crucial early activity is assessing the current state of IT resources against strategic requirements to identify gaps that need to be addressed. (DOI: 10.1007/978-3-319-14547-1)

Question: 22

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:

A new CIO's first priority in establishing effective information governance is to understand the current state of information assets and processes relative to the enterprise's strategic requirements. Performing an information gap analysis is the most comprehensive initial step. This analysis compares the current capabilities ("where we are now") with the business's needs and desired future state ("where we want to be"). The results of this analysis provide a strategic baseline, identify key deficiencies, and form the basis for a roadmap to prioritize all subsequent governance activities, such as valuing assets or reviewing specific procedures.

Why Incorrect Options are Wrong:

A. Quantify the business value of information assets: While essential for risk management and investment decisions, this action is more effective once a baseline understanding of business needs and current information capabilities is established through a gap analysis.
C. Review information classification procedures: This is a specific, tactical activity. A new CIO should first perform a broader strategic assessment (a gap analysis) to determine if classification procedures are a priority area for review.
D. Evaluate information access methods: This is a detailed security and operational task. It is a component of an overall governance framework, not the strategic starting point for a new executive leader.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 1: Governance Framework, Task T1.5, "Identify the gaps between current and future states of the GEIT." The associated knowledge statement, K1.5.1, is "Knowledge of gap analysis." This places gap analysis as a fundamental, early-stage task in establishing and maintaining the governance framework.
2. ISACA, COBIT 2019 Framework: Introduction and Methodology. Chapter 5, "The COBIT Implementation Guide," describes a seven-phase implementation life cycle. Phase 2 is "Where

are we now?" and Phase 3 is "Where do we want to be?". The process of comparing these two phases to identify shortfalls is a gap analysis, which is foundational before moving to Phase 4, "What needs to be done?".

3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer. In Chapter 4, "Implementing Enterprise Governance of IT," the authors describe the implementation life cycle, which begins with recognizing the need to act and assessing the current situation to identify problems and opportunities. This assessment is a precursor to, and a core component of, a gap analysis. (DOI: 10.1007/978-3-319-14547-1)

Question: 23

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:

A business impact analysis (BIA) is the most appropriate tool for this purpose. A BIA systematically identifies critical business processes and quantifies the financial and operational impacts of their disruption over time. This analysis provides a clear monetary value for the risk associated with downtime. By understanding the potential financial loss per hour, day, or week, the IT steering committee can directly compare this quantified risk against the costs of different disaster recovery site options (e.g., hot, warm, cold). This enables a direct, data-driven mapping of cost to risk, facilitating an informed investment decision that aligns recovery expenditure with business criticality.

Why Incorrect Options are Wrong:

A. Key risk indicators (KRIs): KRIs are metrics used to monitor current risk levels against predefined thresholds; they do not quantify the overall financial impact of a potential disaster.
B. Scenario-based assessment: While useful for exploring specific threats, it is often a component of a larger risk assessment and may not provide the comprehensive, business-wide financial quantification that a BIA delivers.
D. Qualitative forecasting: This method relies on subjective expert opinion and lacks the objective, quantifiable financial data required for a robust cost-benefit analysis of a DR site investment.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020), Domain 4: Risk Optimization, Section 4.4, Business Impact Analysis and Business Continuity Plan. The manual states, "The BIA is a key part of the BCP process that identifies the critical business processes... and determines the effect of a disruption on them... This provides the data from which the appropriate recovery strategies can be determined." This directly links the BIA's output to the selection of recovery strategies, which is a cost-versus-risk decision.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018),

Management Objective DSS04 Manage Continuity, Practice DSS04.02 Define business continuity policy, objectives and scope. A key activity listed is to "Perform a business impact analysis (BIA) to identify critical business processes... and the impact of a disruption." The outputs of the BIA are foundational for selecting cost-effective recovery strategies in subsequent practices (e.g., DSS04.03).

3. Tipton, H. F., & Krause, M. (Eds.). (2007). Information Security Management Handbook. Auerbach Publications. Chapter 35, "Business Impact Analysis," explains that the BIA's primary goal is to "correlate specific system components with the critical services they provide, and based on that, to estimate the consequences of a loss of these components." This estimation of consequences (risk) is essential for justifying the cost of recovery solutions. (This is a widely cited academic and professional text in the domain).

Question: 24

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 step to ensure appropriate ownership of access controls after a compliance failure is to link them to a foundational governance structure. An information architecture provides this structure by defining and classifying information assets and, crucially, assigning data owners. By granting access based on this architecture, the enterprise ensures that decisions about who can access sensitive data are made by the designated owners who are accountable for its protection. This directly addresses the root cause of the compliance failure-a lack of clear accountability and ownership-by embedding these principles into the access control process.

Why Incorrect Options are Wrong:

B. Engaging an audit of logical access controls and related security policies
An audit is a reactive measure that identifies existing weaknesses. While valuable for assessment, it does not proactively establish or ensure ownership, which is a core governance function.
C. Implementing multi-factor authentication controls
This is a specific, tactical security control. While it strengthens authentication, it does not address the fundamental governance issue of who is responsible for defining and approving access rights.
D. Authenticating access to information assets based on roles or business rules
This describes an implementation method (e.g., RBAC). For this method to be effective, the roles and rules must be defined and approved by accountable owners, a step which this option omits.

References:

1. ISACA, CGEIT Review Manual, 7th Edition. Domain 4: Information Optimization, Section 2.1 (Information Architecture). The manual explains that a key purpose of an information architecture is to define data ownership and stewardship. This establishes the foundation upon which access controls and other security measures are built, ensuring accountability is clearly assigned.

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. APO14, Managed Data. Practice APO14.01, "Define and maintain a data dictionary and data governance business glossary," emphasizes establishing roles and responsibilities for data, including data owners. Access controls are then based on the policies set by these owners.
3. ISACA, COBIT 2019 Framework: Governance and Management Objectives. DSS05, Managed Security Services. Practice DSS05.04, "Manage user identity and logical access," notes that access rights should be granted based on business need, which is determined and approved by the designated information asset owner. This confirms that ownership precedes the granting of access.

Question: 25

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 the foundational document that formally defines the principles, values, and desired behaviors for the entire organization. To effectively incorporate these behaviors into the IT governance framework, the framework must align with and be guided by this code. The code of ethics sets the "tone at the top" and provides the overarching principles that should permeate all IT processes, decisions, and activities. This ensures that IT culture is a direct extension of the desired enterprise culture, which is a critical success factor for effective Enterprise Governance of IT (EGIT).

Why Incorrect Options are Wrong:

B. Risk mitigation strategies and action plans are tactical responses to specific identified risks, not a comprehensive guide for all desired organizational behaviors.
C. Documented consequences for noncompliance are an enforcement mechanism; they address what happens when desired behaviors are not followed, but do not define the desired behaviors themselves.
D. An enterprise RACI matrix defines roles and responsibilities within processes. It clarifies who does what, but does not specify the ethical or behavioral standards for performing those duties.

References:

1. ISACA, COBIT 2019 Framework: Introduction and Methodology, 2018, p. 31. The framework identifies "Culture, ethics and behavior" as one of the seven core components of a governance system, stating it is a critical success factor. An enterprise code of ethics is the primary instrument for defining this component.
2. ISACA, CGEIT Review Manual, 8th Edition, 2020, Domain 1, Section 1.6, "Organizational Structures, Roles, and Responsibilities." This section emphasizes the board's responsibility for establishing an ethical culture and notes that a code of ethics is a key tool for communicating and embedding these values throughout the enterprise, including its IT functions.

3. ISACA, CGEIT Review Manual, 8th Edition, 2020, Domain 1, Section 1.9, "Policies and Procedures." This section clarifies that policies, which are core to any governance framework, should be derived from the enterprise's guiding principles and ethical stance, as articulated in documents like a code of ethics.

Question: 26

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:

For performance measures to be effective in improving organizational performance, they must be relevant and accepted by the stakeholders who will use them. If stakeholders do not find the measures meaningful or do not agree with their validity, the measures will fail to drive the desired behaviors or inform strategic decisions. Acceptance ensures buy-in and accountability, while meaningfulness ensures the measures are directly linked to strategic objectives and actionable insights, which is the ultimate purpose of performance measurement in enterprise governance.

Why Incorrect Options are Wrong:

A. Benchmarking is a valuable technique for setting targets and providing context, but it is not a mandatory prerequisite for developing appropriate, internally focused performance measures.
C. While measures should be based on reliable data, the definition of an appropriate measure comes first. This may necessitate the creation of new data sources, not just reliance on existing ones.
D. Approval by the IT steering committee is a governance formality, often limited to IT-related measures. It does not inherently make a measure appropriate or meaningful for broader organizational performance.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 4: Value Optimization, Section 2.3, Value Delivery Monitoring. The manual emphasizes that performance metrics must be linked to business objectives and be meaningful to the business to ensure value is being delivered and monitored effectively.
2. ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. Section 3.2, The COBIT Goals Cascade. The framework illustrates that the entire governance system, including performance metrics, is derived from stakeholder needs and enterprise goals, reinforcing that measures must be meaningful to those stakeholders.

3. Kaplan, R. S., & Norton, D. P. (1992). The Balanced Scorecard-Measures That Drive Performance. Harvard Business Review, 70(1), 71-79. This foundational academic work on performance measurement argues that for measures to be effective, they must translate high-level strategy into terms that are understandable and actionable for the organization's employees (stakeholders).

Question: 27

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:

The first strategic step for IT governance when considering a major initiative, such as a new line of business, is to ensure all stakeholders agree on a vision for the future state. This shared vision establishes the high-level direction, purpose, and desired outcome of the change. It serves as the foundational element upon which all subsequent strategic activities, such as defining goals, objectives, and metrics, are built. Without a unified vision, efforts to align IT with business strategy will be fragmented and ineffective, jeopardizing the success of the new venture. This initial alignment is a core principle of enterprise governance of IT.

Why Incorrect Options are Wrong:

A. Objectives are specific, measurable actions derived from broader goals and the overall vision. They are defined after the vision is established, not before.
B. Metrics are developed to measure the achievement of objectives. This is a subsequent step in the planning and performance management process, not the initial strategic one.
D. A change response plan is a tactical component of change management, addressing the implementation phase. It is created much later, after the strategic direction is set.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 1: Governance of Enterprise IT, Section 1.4, Strategic Planning. The manual emphasizes that strategic planning begins with defining the enterprise's mission and vision, which then drives the formulation of goals and objectives. The vision provides the "what" before the "how."
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. APO02 Manage Strategy. The description for practice APO02.01, "Understand enterprise context and direction," states the need to "Consider the current and future business environment... to help formulate the enterprise's long-term vision and mission." This understanding of the future state is a prerequisite

for developing the IT strategy.
3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 3, "IT Governance Mechanisms," discusses how strategic alignment starts with a shared understanding between business and IT executives about the future direction, which is encapsulated in the vision. (DOI: 10.1007/978-3-319-14547-1).

Question: 28

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:

The fundamental principle of the governance of enterprise IT (GEIT) is to ensure that IT investments align with and support the enterprise's strategic objectives to create business value. Therefore, the primary consideration when prioritizing IT projects must be the impact they will have on the business. This holistic view encompasses strategic alignment, potential return on investment, risk mitigation, and contribution to overall enterprise goals. Prioritizing based on business impact ensures that resources are allocated to the initiatives that will deliver the most significant value, rather than focusing on narrower criteria.

Why Incorrect Options are Wrong:

A. Technical capability is a critical feasibility and risk assessment factor, but it is secondary to the project's potential business value.
B. Process owner expectations are a valuable input for assessing operational benefits, but prioritization must consider the entire enterprise's strategic objectives, not just one area.
C. IT performance benchmarks against competitors provide context and can identify opportunities, but they are not the primary driver for prioritization, which must be based on internal strategic goals.

References:

1. ISACA, CGEIT Review Manual, 8th Edition, 2020. Domain 3: Benefits Realization, Section 3.2, "IT Portfolio Management," emphasizes that the investment portfolio must be aligned with the enterprise's strategic objectives and that prioritization is based on the potential to add value to the business.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2018. Governance Objective EDM02, "Ensured Benefits Delivery," Practice EDM02.02, states the need to "Direct value optimization by prioritizing investment programs based on their potential contribution to strategic objectives and the enterprise value." (p. 43).

3. ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2018. Management Objective APO05, "Managed Portfolio," Practice APO05.03, states, "Prioritize, select and defer programs and other investments based on evaluation of their alignment with enterprise strategy, their business value and risk." (p. 78).

Question: 29

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:

The question highlights a critical risk factor: the enterprise has no experience with cloud technology. The most immediate and effective first step to mitigate the risk of service disruption is to address this knowledge gap. Engaging an experienced IT consultant provides the necessary expertise to guide the organization through the entire migration process. This expert guidance is foundational, ensuring that subsequent steps like evaluating sourcing options, updating the enterprise architecture, and defining performance indicators are performed correctly and based on informed decisions, thereby minimizing the risk of failure or disruption.

Why Incorrect Options are Wrong:

A. Implementing key performance indicators (KPIs) is a step to measure success and manage performance, which occurs after a strategy and solution have been selected, not as the initial risk mitigation action.
B. Reflecting the change in the enterprise architecture (EA) is a necessary step, but attempting it without the required expertise is itself a risk. The expertise must be acquired first to inform the EA changes.
C. Evaluating sourcing options (e.g., cloud vendors, service models) requires deep technical and commercial knowledge. Making this critical decision without experience would be a high-risk endeavor.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 3: Resource Optimization, Task Statement 3.3, emphasizes ensuring sufficient and appropriate resources to support objectives. When internal skills are absent for a strategic initiative, sourcing external expertise is a primary method for resource optimization and risk reduction.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The management

objective APO07 Managed Human Resources includes practice APO07.02, "Sustain a skilled and motivated workforce," which states that organizations should "Provide for the acquisition of new skills as required by enterprise goals," including sourcing them externally. For a major technology shift like cloud migration, this is a prerequisite for success.

3. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The management objective BAI05 Managed Organizational Change highlights the need to prepare stakeholders for change. A key component is ensuring the organization is equipped with the necessary skills and knowledge, which often involves bringing in external experts to guide the transition and mitigate risks associated with inexperience.

Question: 30

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:

The role of a data steward is to manage and oversee an organization's data assets on behalf of business stakeholders. This includes responsibility for data quality, data definition, and resolving data issues. Data normalization is a process to improve data integrity and minimize redundancy. When duplicate data items are found, it signifies a data quality issue. The data steward is the designated role responsible for investigating such issues, defining the correct data structure, and overseeing the remediation process, which includes normalization.

Why Incorrect Options are Wrong:

A. Business system owner: This role is accountable for the system's overall business value and functionality, but typically delegates the operational responsibility for data quality and definition to data stewards.
C. Database administrator (DBA): The DBA is a technical role focused on the database's performance, security, and availability. They would implement the technical changes for normalization but are not responsible for defining the data rules.
D. Application manager: This role is responsible for the day-to-day operation of the application, not the governance and quality of the underlying data assets, which is the purview of data stewardship.

References:

1. ISACA, CGEIT Review Manual, 8th Edition (2020). Domain 2: IT Resources, Section B: Information/Data. The manual describes the data steward as being "responsible for the quality of defined data elements," which directly encompasses the task of resolving duplicates through normalization. The distinction is made between the data owner (accountable) and the data steward (responsible).
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018). APO14

Managed Data, APO14.03: "Define and maintain data and information architecture." This practice includes establishing roles and responsibilities for data management. The framework's supporting guidance consistently assigns the responsibility for data quality and definition to a stewardship function.
3. Soares, S. (2015). Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program. MC Press. Chapter 4, "Data Governance Roles and Responsibilities," clearly defines the Data Steward as the individual with day-to-day responsibility for managing the quality, integrity, and definitions of specific data assets. This includes activities like identifying and resolving data redundancy. (Note: While a book, this is a foundational text in the field, often referenced in academic and professional contexts related to ISACA's body of knowledge).

Question: 31

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:

The primary function of a board-level IT strategy committee is to provide governance and oversight, ensuring that the IT strategy directly supports and enables the enterprise's overall strategic objectives. This committee acts as a bridge between the board and executive management, advising the board on IT-related matters and ensuring that IT-enabled investments are aligned with business goals to deliver value. This oversight role is fundamental to the principle of strategic alignment in the governance of enterprise IT (GEIT).

Why Incorrect Options are Wrong:

B: Managing IT risk is a key governance activity, but it is often the focus of a dedicated risk committee or the board as a whole, not the primary charter of a strategy committee.
C: Driving development and implementation are management functions, typically led by the CIO and IT executives, whereas the committee's role is governance and oversight.
D: The full board of directors retains ultimate governance accountability for the overall business strategy; this responsibility cannot be delegated to a subcommittee.

References:

1. ISACA. (2020). CGEIT Review Manual, 8th Edition. Domain 1: Governance of Enterprise IT, Section 1.7, Governance Structures, Organizational Structures, and Roles and Responsibilities. This section describes the role of board-level committees, emphasizing that an IT strategy committee's main purpose is to advise the board and ensure alignment between enterprise and IT strategy.
2. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Governance Objective EDM02: Ensure Benefits Delivery. This objective details the board's responsibility for directing value optimization, a task facilitated by an IT strategy committee that ensures IT-enabled initiatives are aligned with enterprise strategy.
3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information

Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 3, "Structures, Processes and Relational Mechanisms," pp. 59-61. This academic text explicitly states that the IT strategy committee is a key structure for achieving business/IT alignment by providing input and oversight. (DOI: 10.1007/978-3-319-14547-1)

Question: 32

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:

The question describes a scenario where risk identification, the first step in the risk management process, has been completed. According to established governance and risk management frameworks, the immediate next step is risk analysis. This involves assessing the identified threats to determine their likelihood of occurrence and the potential impact on business objectives and assets, such as the data center. This analysis provides the necessary information to prioritize risks and make informed decisions about subsequent risk responses. Without first understanding the probability and magnitude of the threat, any action taken would be premature and potentially misaligned with the enterprise's risk appetite.

Why Incorrect Options are Wrong:

A. Implementing a warning system is a risk response (mitigation) action. Such actions are decided upon only after the risk has been properly analyzed and evaluated.
C. Relocating the data center is a risk response (avoidance) strategy. This is a significant decision that would only be justified after a thorough risk assessment demonstrates an unacceptably high level of risk.
D. Assessing existing protections is part of a detailed risk analysis, but the foundational step is to first understand the inherent likelihood and impact of the threat itself.

References:

1. ISACA, The Risk IT Framework, 2nd Edition (2020): The framework outlines the risk management process. The process domain Risk Evaluation (RE) starts with RE1 Collect Data, followed by RE2 Analyze Risk. RE2.2 states, "Estimate the frequency and/or probability and the magnitude of the business impact for risk scenarios." This directly corresponds to assessing likelihood and impact immediately after identification. (Page 49, RE2 Analyze Risk).
2. ISACA, CGEIT Review Manual, 8th Edition (2020): Domain 2, IT Risk Optimization, describes the risk management life cycle. It emphasizes that after risk identification, the next phase is risk

analysis, which "involves assigning a value to the risk in terms of likelihood and impact." (Domain 2, Section 2.5, Risk Analysis and Evaluation).
3. ISACA, COBIT 2019 Framework: Governance and Management Objectives (2018): The management objective APO12 Manage Risk details the risk management process. Practice APO12.03 Analyze risk follows APO12.02 Collect data. APO12.03 includes key activities such as "Estimate the likelihood and impact of all identified risk scenarios." (Page 103, APO12.03).

Question: 33

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:

IT governance ensures that IT activities align with business objectives and establishes clear accountability. Data is a critical business asset, and its business process owners are ultimately accountable for its integrity, quality, and fitness for purpose. Mandating documented approval from these owners before a data transition is a fundamental governance checkpoint. This approval signifies that the business has reviewed and accepted the migration plan, conversion rules, and success criteria, ensuring the new platform will meet business requirements and formally acknowledging the transfer of this critical asset.

Why Incorrect Options are Wrong:

B. Data conversion in a test environment is a critical operational task to ensure technical correctness, but it is a means to an end, not the overarching governance mandate itself.
C. Using control totals is a specific control procedure to verify data completeness during migration. It is a detailed technical activity, not a high-level governance prerequisite.
D. A crisis management plan is an important risk management component for the overall project, but the most direct and fundamental governance mandate concerning the data is approval from its business owner.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 2: IT Resources, Section 2.3.4, Information/Data. This section emphasizes that data owners are responsible for the quality of data and for approving access. This responsibility extends to approving the migration of data to a new platform. Task Statement 2.8 states to "Ensure that the roles, responsibilities, and accountabilities for information are defined and assigned," which underpins the authority of the data owner to provide such approval.
2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The management objective BAI07 Managed IT Change Acceptance and Transitioning includes the key practice

BAI07.05, "Obtain formal acceptance of the new or changed solution from business and IT." This formal acceptance must come from stakeholders, critically including the business process and data owners, before the solution goes live.
3. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The management objective APO14 Managed Data includes practice APO14.02, "Define and implement data management and governance roles and structures." This practice establishes the role of the data owner, who has the authority and accountability to make decisions about data, including its transition between systems.

Question: 34

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:

The balanced scorecard (BSC) is a strategic performance management framework designed to translate an organization's strategy into a set of measurable performance objectives. An IT balanced scorecard specifically links IT strategy to business strategy across four key perspectives: financial, customer, internal processes, and learning and growth. By defining metrics and targets for each perspective that are directly tied to business goals, the BSC provides a comprehensive and clear view of how IT activities are contributing to business priorities. This makes it the most effective tool for demonstrating the current state of strategic alignment to the CIO.

Why Incorrect Options are Wrong:

A. IT maturity model: This assesses the capability and sophistication of IT processes, not their direct alignment with specific, current business objectives.
B. Business case: A business case justifies a single proposed project or investment; it does not provide a holistic view of the overall, current alignment status.
D. IT investment status: This reports on the financial health (e.g., budget versus actuals) of IT investments, which does not inherently measure their strategic value or alignment.

References:

1. ISACA, CGEIT Review Manual, 8th Edition. Domain 1: Governance of Enterprise IT, Section 1.9, "Strategic Planning and the Use of Frameworks." The manual describes the balanced scorecard as a key performance management tool used to "translate strategy into operational objectives that drive both behavior and performance." It emphasizes its role in linking IT goals to enterprise goals.
2. Van Grembergen, W., & De Haes, S. (2009). Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value. Springer. Chapter 4, "Implementing IT Governance using the IT Balanced Scorecard," details how the IT BSC is used to measure the

contribution of IT to the business, thereby demonstrating alignment. It states, "The IT balanced scorecard is an ideal instrument to measure and manage the IT department's strategy and its alignment with the business strategy" (p. 95).
3. ISACA, COBIT 2019 Framework: Introduction and Methodology. Section 3.3, "Goals Cascade." While not naming the BSC directly in this section, the entire concept of the goals cascade-translating stakeholder needs into enterprise goals, then into alignment goals, and finally into governance and management objectives-is the foundational principle upon which the balanced scorecard operates to ensure and demonstrate alignment. The BSC is a primary tool for operationalizing the goals cascade.

Question: 35

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:

The balanced scorecard (BSC) is a strategic performance management framework used to provide a comprehensive, high-level view of performance to senior leadership, such as the board of directors. It translates IT strategy into a set of performance measures across multiple perspectives-typically financial, customer, internal processes, and learning/growth. This approach ensures that the reporting is not limited to just technical or financial metrics but presents a holistic and "balanced" picture of IT's contribution to business objectives, which is precisely what a board requires for strategic oversight.

Why Incorrect Options are Wrong:

B. Key risk indicators (KRIs): These are metrics focused specifically on risk exposure and provide early warnings of potential issues, not a comprehensive view of overall performance.
C. Maturity model: This tool assesses the capability and sophistication of processes at a point in time, rather than measuring ongoing operational and strategic performance.
D. Key performance indicators (KPIs): While a balanced scorecard uses KPIs, a list of individual KPIs lacks the strategic context and multi-perspective framework that a BSC provides for an overall view.

References:

1. ISACA, CGEIT Review Manual, 8th Edition, 2020. Domain 4: Value Optimization, Section 4.3, Task V4.4 (Monitor and Report on the Performance of the IT Investment Portfolio), discusses the use of the IT balanced scorecard as a primary tool for measuring and communicating IT's business value to stakeholders, including the board.
2. ISACA, COBIT 2019 Framework: Introduction and Methodology, 2018. Chapter 4, "The COBIT Goals Cascade," describes how enterprise goals are translated into IT-related goals using dimensions that mirror the balanced scorecard (Financial, Customer, Internal, and Growth), establishing it as a foundational concept for governance reporting (p. 31).

3. Van Grembergen, W., & De Haes, S. (2009). Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value. Springer. The book extensively details the IT balanced scorecard as a critical mechanism for performance measurement in IT governance, specifically for communicating value and performance to executive management and the board (Chapter 4).