[Mar-2025 Verified ISACA CGEIT Bundle Real Exam Dumps PDF [Q293-Q313

[Mar-2025] Verified ISACA CGEIT Bundle Real Exam Dumps PDF
CGEIT Dumps PDF New [2025] Ultimate Study Guide

Achieving the CGEIT certification demonstrates a professional's commitment to excellence in IT governance and their ability to provide value to their organization. It is a valuable credential for those seeking to advance their career in IT governance, risk management, and compliance. Certified in the Governance of Enterprise IT Exam certification is recognized by organizations around the world and is a testament to an individual's expertise in the field of enterprise IT governance.

NO.293 An enterprise is initiating efforts to improve system availability to mitigate IT risk to the business. Which of the following results would be MOST important to report to the CIO to measure progress?
* Incident severity and downtime trend analysis
* Probability and seventy of each IT risk
* Financial losses and bad press releases
* Customer and stakeholder complaints over time
Incident severity and downtime trend analysis is the most important result to report to the CIO to measure progress in improving system availability to mitigate IT risk to the business, because it directly reflects the impact and frequency of system failures or

disruptions on the business operations, processes, and functions. By analyzing the severity and duration of incidents over time, the CIO can evaluate the effectiveness of the IT risk management and system availability strategies, and identify any gaps, issues, or opportunities for improvement. Incident severity and downtime trend analysis can also help the CIO to communicate the value and performance of the IT risk management and system availability initiatives to the business stakeholders, and justify any further investment or action required to achieve the desired outcomes.

The other options are not as important as incident severity and downtime trend analysis, because they are either too indirect or too subjective to measure progress in improving system availability to mitigate IT risk to the business. Probability and severity of each IT risk is a useful input for IT risk management, but it does not necessarily reflect the actual occurrence or impact of system failures or disruptions on the business1. Financial losses and bad press releases are possible consequences of system failures or disruptions, but they may not capture the full extent or root causes of the IT risk to the business2. Customer and stakeholder complaints over time are indicators of customer satisfaction and loyalty, but they may not be reliable or consistent measures of system availability or IT risk to the business

NO.294 Which of the following techniques is used for understanding the &#8220;environment&#8221; in which a business operates?
* Critical success factor analysis
* PEST analysis
* SWOT analysis
* Market segmentation
Section: Volume B

NO.295 Which of the following is the GREATEST impact to an enterprise that has ineffective information architecture?
* Poor desktop service delivery
* Data retention
* Redundant systems
* Poor business decisions
Information architecture (IA) is the practice of structuring and presenting the parts of something &#8211; whether that&#8217;s a website, mobile app, blog post, book, or brick-and-mortar store &#8211; to users so that it&#8217;s easy to understand. IA can help users find information and complete tasks1.

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

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

* If the enterprise&#8217;s website has a confusing or inconsistent navigation system, users may not be able to find the information they need or want, such as product details, prices, reviews, or contact information. This can result in lower customer satisfaction, engagement, conversion, and retention14.

* If the enterprise&#8217;s data is stored in multiple systems or platforms that are not integrated or interoperable, users may not be able to access or share the data across different departments or functions. This can result in data silos, duplication, inconsistency, or incompleteness25.

* If the enterprise&#8217;s data is not labeled or categorized properly, users may not be able to search or filter the data effectively. This can result in data overload, irrelevance, or obscurity25.

* If the enterprise&#8217;s data is not governed or managed properly, users may not be able to trust or verify the

* data quality or integrity. This can result in data errors, inaccuracies, or biases25.

Therefore, an enterprise that has ineffective information architecture may have poor business decisions as its greatest impact. References: Information Architecture Basics | Usability.gov. The Importance of Information Architecture to UX Design. How Enterprise Architecture Can Help You Eliminate Technical Debt. What Is Information Architecture & Why Does It Matter? &#8211; HubSpot Blog. Why Do We Need Information Architecture &#8211; Architecture.

NO.296 An IT risk assessment for a large healthcare group revealed an increased risk of unauthorized disclosure of information. Which of the following should be established FIRST to address the risk?
* Data encryption tools
* Data loss prevention tools
* Data classification policy
* Data retention policy
The first step to address the risk of unauthorized disclosure of information is to establish a data classification policy. A data classification policy defines the categories of data based on their sensitivity and value to the organization, and specifies the appropriate security controls and handling procedures for each category. A data classification policy helps to identify the most critical and confidential data, and to prioritize the protection of such data from unauthorized access, disclosure, modification, or loss. A data classification policy also provides a basis for implementing other measures, such as data encryption tools, data loss prevention tools, and data retention policy, to enhance the security of data. References := Reducing Cybersecurity Security Risk From and to Third Parties; Unauthorized Access: Prevention Best Practices; Security of Enterprise Application Integration

NO.297 Which of the following activity loops emphasizes on monitoring and deciding processes?
* Loop 2
* Loop 4
* Loop 3
* Loop 1

NO.298 An airline wants to launch a new program involving the use of artificial intelligence (Al) and machine learning the mam objective of the program is to use customer behavior to determine new routes and markets Which of the following should be done NEXT?
* Consult with the enterprise privacy function
* Define the critical success factors (CSFs)
* Present the proposal to the IT strategy committee
* Perform a business impact analysis (BIA)
Critical success factors (CSFs) are the essential elements or conditions that must be achieved for a project or program to be successful. CSFs help to define the scope, objectives, and expected outcomes of the project or program, as well as the key performance indicators (KPIs) and metrics to measure and evaluate the progress and results. CSFs also help to align the project or program with the strategic goals and vision of the organization, and to communicate the value proposition and benefits to the stakeholders. Therefore, before launching a new program involving the use of artificial intelligence (AI) and machine learning, an airline should define the CSFs to ensure that the program is feasible, desirable, and viable, and that it meets the business needs and expectations of the customers and the market. Reference:= CGEIT Review Manual, Chapter 1: Framework for the Governance of Enterprise IT, Section 1.2: GEIT Principles, Subsection 1.2.3: Principle 3: Ensure Outcomes Are Delivered Through Effective Use of IT, Page 28.

NO.299 Which of the following should be done FIRST when defining responsibilities for ownership of information and systems?
* Require an information risk assessment.
* Identify systems that are outsourced.
* Ensure information is classified.
* Require an inventory of information assets.

The FIRST step when defining responsibilities for ownership of information and systems is to require an inventory of information assets. An information asset is any data, device, or other component of the environment that supports information-related activities1. An inventory of information assets is a comprehensive list of all the information assets that an organization owns, controls, or uses2. By creating an inventory of information assets, an organization can:

Identify the types, locations, formats, and volumes of information assets3 Determine the value, sensitivity, and criticality of information assets4 Assign ownership and accountability for information assets5 Establish appropriate security controls and protection measures for information assets6 Monitor and audit the usage and lifecycle of information assets7 The other options are not as important as option D. While it is important to require an information risk assessment, identify systems that are outsourced, and ensure information is classified, these are subsequent steps that depend on the availability and accuracy of the inventory of information assets. Without an inventory of information assets, it would be difficult to perform a risk assessment, identify outsourced systems, or classify information according to its value and sensitivity. Reference:= Information Asset &#8211; an overview | ScienceDirect Topics1 Information Asset Inventory &#8211; NIST CSRC2 How to Create an Information Asset Inventory &#8211; Infosec Resources3 Information Asset Valuation: A Methodology &#8211; ISACA4 Data Ownership: Considerations for Risk Management &#8211; ISACA5 Information Asset Protection &#8211; NIST CSRC6 Information Asset Management &#8211; NIST CSRC7

NO.300 An enterprise&#8217;s decision to move to a virtualized architecture will have the GREATEST impact on:
* system life cycle management.
* asset classification.
* vendor management
* vulnerability management.
Moving to a virtualized architecture will have the greatest impact on vendor management, as it will require the enterprise to select, contract, and monitor the performance of the cloud or virtualization service providers. Vendor management is essential for ensuring that the virtualized architecture meets the enterprise&#8217;s requirements, standards, and expectations, as well as for managing the risks, costs, and benefits of the virtualization strategy. Vendor management also involves negotiating and enforcing service level agreements (SLAs), ensuring compliance with regulations and policies, and resolving any issues or disputes that may arise with the vendors.

System life cycle management, asset classification, and vulnerability management are also important aspects of IT governance, but they are not as significantly affected by moving to a virtualized architecture as vendor management. System life cycle management is the process of planning, developing, testing, deploying, maintaining, and retiring IT systems. Asset classification is the process of identifying, categorizing, and labeling IT assets based on their value, sensitivity, and criticality. Vulnerability management is the process of identifying, assessing, prioritizing, and mitigating IT vulnerabilities that may pose a threat to the enterprise&#8217;s security or operations. These processes may need to be adapted or updated to accommodate the virtualized architecture, but they are not fundamentally changed by it.

NO.301 An enterprise is about to complete a major acquisition, and a decision has been made that both companies will be using the parent company&#8217;s IT infrastructure. Which of the following should be done NEXT?
* Update the enterprise architecture (EA).
* Perform a business impact analysis (BIA.
* Conduct a gap analysis.
* Develop a communication plan to support the merger.
A gap analysis is the process of comparing the current state and the desired state of an organization or a system, and identifying the gaps or differences between them1. A gap analysis can help to determine the actions and resources needed to bridge the gaps and achieve the desired outcomes2. In the context of an IT infrastructure integration after a major acquisition, a gap analysis can help to:

Assess the compatibility and interoperability of the IT systems, applications, data, and processes of both companies3 Identify the gaps, risks, issues, and opportunities related to the IT infrastructure integration4 Prioritize and plan the IT infrastructure integration activities and projects5 Align the IT infrastructure integration with the business goals and objectives of the acquisition Therefore, conducting a gap analysis should be done NEXT after deciding that both companies will be using the parent company&#8217;s IT infrastructure.

The other options are not as important as option C. While it is important to update the enterprise architecture (EA), perform a business impact analysis (BIA), and develop a communication plan to support the merger, these are subsequent steps that can be done after conducting a gap analysis. A gap analysis can provide valuable inputs and insights for these steps, such as the current and target EA, the potential impacts of the IT infrastructure integration on the business operations and stakeholders, and the communication needs and channels for the IT infrastructure integration. References := What is Gap Analysis? Definition, Methodology & Examples | ASQ1 Gap Analysis: How to Bridge the Gap Between Performance and &#8230;2 How to Make a Successful IT Integration Strategy for Mergers and &#8230;4 M&A: The Six Phases of IT Integration &#8211; Interlink Cloud Blog3 Post-Merger Integration: M&A Integration Process Guide &#8211; DealRoom5 Success Factors for Integrating IT Systems After a Merger | CIO

NO.302 Prior to decommissioning an IT system, it is MOST important to:
* assess compliance with environmental regulations.
* assess compliance with the retention policy.
* review the media disposal records.
* review the data sanitation records.

This is because before decommissioning an IT system, it is most important to ensure that the data stored on the system is handled according to the retention policy of the organization. A retention policy is a document that specifies how long and where different types of data should be kept, archived, or deleted, based on the business, legal, and regulatory requirements. Assessing compliance with the retention policy can help to avoid data loss, leakage, or breach, as well as comply with the applicable laws and regulations.

Assessing compliance with environmental regulations is not the most important action, as it is a secondary consideration for decommissioning an IT system. Environmental regulations are rules that govern the disposal or recycling of IT equipment and materials, such as batteries, cables, or monitors, in order to protect the environment and human health. Assessing compliance with environmental regulations can help to reduce the environmental impact and waste of IT resources, as well as avoid fines or penalties. However, assessing compliance with environmental regulations does not address the primary concern of data management and security.

Reviewing the media disposal records is not the most important action, as it is a subsequent step after assessing compliance with the retention policy. Media disposal records are documents that provide evidence and verification of the proper disposal or destruction of IT media, such as hard drives, tapes, or disks, that contain sensitive or confidential data. Reviewing the media disposal records can help to ensure that the data on the IT system is erased or overwritten in a secure and irreversible manner, as well as comply with the audit and accountability requirements. However, reviewing the media disposal records does not provide a comprehensive assessment or guidance for data retention and compliance.

Reviewing the data sanitation records is not the most important action, as it is a similar step to reviewing the media disposal records. Data sanitation records are documents that provide evidence and verification of the proper sanitation or cleansing of data on an IT system, such as deleting, encrypting, or masking data that is no longer needed or relevant. Reviewing the data sanitation records can help to ensure that the data on the IT system is protected from unauthorized access, disclosure, modification, or destruction, as well as comply with the privacy and confidentiality requirements. However, reviewing the data sanitation records does not provide a thorough assessment or guidance for data retention and compliance.

NO.303 Senior management is reviewing the results of a recent security incident with significant business impact. Which of the following findings should be of GREATEST concern?
* Significant gaps are present m the incident documentation.
* The incident was not logged in the ticketing system.
* Response decisions were made without consulting the appropriate authority.
* Response efforts had to be outsourced due to insufficient internal resources.

The finding that should be of greatest concern to senior management is that response decisions were made without consulting the appropriate authority. This is because response decisions are critical actions that can affect the outcome and impact of a security incident, and they should be made by the designated authority who has the responsibility and accountability for the incident response. According to CISA, the Department of Justice, through the FBI and the NCIJTF, is the lead agency for threat response during a significant incident, with DHS&#8217;s investigative agencies-the Secret Service and ICE/HSI &#8211; playing a crucial role in criminal investigations1. If response decisions are made without consulting the appropriate authority, it may result in:

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

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

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

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

NO.304 Which of the following is the PRIMARY role of the CEO in IT governance?
* Evaluating return on investment
* Managing the risk governance process
* Establishing enterprise strategic goals
* Nominating IT steering committee membership
Explanation/Reference: https://corporatefinanceinstitute.com/resources/careers/jobs/what-is-a-ceo-chief-executive-officer/

NO.305 An enterprise is contracting with an outsourcing partner for a long-term engagement. The BEST time for the enterprise to plan for the event of contract termination:
* developing the initial contract.
* either party decides to terminate the contract.
* issues surface in the contractual relationship.
* planning for the contract as part of business continuity.

NO.306 Which of the following types of agreement creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret?
* CNC
* NDA
* SLA
* Non-price competition

NO.307 Which of the following components of the COSO ERM identifies the required information, captures it, and communicates it in a form and time frame that enable people to carry out their responsibilities?
* Information and communication
* Internal environment
* Monitoring
* Objectives setting

NO.308 Which of the following BEST helps to ensure that IT policies are

aligned with organizational strategies?
* The policies are approved by the board of directors.
* The policies are developed using a top-down approach.
* The policies are updated annually.
* The policies are periodically audited.

Ensuring that IT policies are aligned with organizational strategies is best achieved when the policies are developed using a top-down approach. This approach starts with strategic objectives and cascades down to operational policies, ensuring coherence and alignment with the overall direction and goals of the organization. While board approval, annual updates, and periodic audits are important for policy governance, the top-down development approach ensures that policies are inherently designed to support organizational strategies from the outset.

NO.309 Besides the mitigation of IT risk, which of the following is the PRIMARY outcome of IT governance?
* Control of IT processes
* Meeting of IT financial goals
* Resolution of IT audit findings
* Value delivery of IT to the business

Explanation/Reference: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/InteligenciaFrentealRiesgo/No.6-RiskIntelligenceCIO.pdf

NO.310 Which of the following functions of HR department is liable for attitude surveys, labor relation, employee handbook, and labor law compliance?
* Personnel policy
* Employee relation
* Compensation and benefit
* Analysis and design for work

Section: Volume C

NO.311 Which of the following areas tracks the project delivery, and monitors the IT services?
* Risk management
* Performance measurement
* Strategic alignment
* Value delivery

Section: Volume C

NO.312 The BEST way to manage an outsourced vendor relationship is by:
* conducting periodic risk assessments.
* reviewing annual independent third-party reports.
* providing clear objectives and transparency.
* analyzing performance statistics from the vendor.

Providing clear objectives and transparency is the best way to manage an outsourced vendor relationship, because it ensures that both parties have a common understanding of the expectations, deliverables, and outcomes of the outsourcing arrangement. By providing clear objectives, the client can communicate the business goals, needs, and requirements to the vendor, and the vendor can align their services, processes, and resources accordingly. By providing transparency, the client can share relevant information, feedback, and insights with the vendor, and the vendor can report on their performance, issues, and risks regularly. Providing clear objectives and transparency can also foster trust, collaboration, and innovation between the client and the vendor, and help resolve any conflicts or disputes that may arise. According to Outsourcing Vendor Best Practices: 5 Tips for a Successful Relationship, &#8220;Transparency is critical to a successful outsourcing relationship. It helps to ensure that both parties are on the same page regarding expectations, deliverables and performance.&#8221;

NO.313 The board of directors of a large organization has directed IT senior management to improve IT governance within the organization. IT senior management&#8217;s MOST important course of action should be to:
* understand the driver that led to a desire to change.
* assess the current slate of IT governance within the organization.
* review IT strategy and direction.
* analyze IT service levels and performance.
The most important course of action for IT senior management to improve IT governance within the organization is to understand the driver that led to a desire to change. IT governance is the process of ensuring that IT supports and enables the achievement of the enterprise&#8217;s goals and objectives, and delivers value to the stakeholders1. IT governance is influenced by various internal and external factors, such as business strategy, customer expectations, regulatory requirements, industry standards, best practices, and emerging technologies1. Therefore, before initiating any improvement initiatives, IT senior management should first identify and analyze the driver that prompted the board of directors to request a change in IT governance. This will help them to understand the current situation, the desired state, the gap between them, and the rationale and urgency for improvement2. By understanding the driver that led to a desire to change, IT senior management can also align their improvement efforts with the board&#8217;s vision and expectations, communicate the benefits and challenges of change, and gain their support and commitment2. Reference: CGEIT Review Manual (Digital Version) or CGEIT Review Manual (Print Version), Chapter 1: Governance of Enterprise IT, Section 1.1: IT Governance Frameworks and Principles, Page 9-10. What is CGEIT? A certification for seasoned IT governance professionals.

Pass Your ISACA Exam with CGEIT Exam Dumps: https://www.braindumpsit.com/CGEIT_real-exam.html]