Number: CISA
Passing Score: 800
Time Limit: 120
File Version: 51.0

Exam Code: CISA
Exam Name: Certified Information Systems Auditor

Exam A

QUESTION 1
A disaster recovery plan (DRP) should include steps for:

A. assessing and quantifying risk.
B. negotiating contracts with disaster planning consultants.
C. identifying application control requirements.
D. obtaining replacement supplies.

Correct Answer: D
Section:
Explanation:
A disaster recovery plan (DRP) is a set of detailed, documented guidelines that outline a business' critical assets and explain how the organization will respond to unplanned incidents.Unplanned incidents or disasters typically include cyberattacks, system failures, power outages, natural disasters, equipment failures, or infrastructure damage1. A DRP aims to minimize the impact of a disaster on the business continuity, data integrity, and service delivery of the organization. A DRP also helps the organization recover from a disaster as quickly and efficiently as possible.
A DRP should include steps for obtaining replacement supplies, as this is an essential part of restoring the normal operation of the organization after a disaster. Replacement supplies may include hardware, software, data, network components, office equipment, or other resources that are needed to resume the business functions and processes that were disrupted by the disaster. Obtaining replacement supplies may involve contacting vendors, suppliers, or partners; activating backup or alternative systems; or purchasing or renting new equipment. A DRP should identify the sources, locations, and costs of the replacement supplies, as well as the procedures and responsibilities for acquiring and installing them.
The other three options are not steps that a DRP should include, as they are either part of the pre-disaster planning process or not directly related to the disaster recovery objectives.Assessing and quantifying risk is a step that should be done before creating a DRP, as it helps identify the potential threats and vulnerabilities that could affect the organization and determine the likelihood and impact of each scenario2.Negotiating contracts with disaster planning consultants is also a pre-disaster activity that may help the organization design, implement, test, and maintain a DRP with external expertise and guidance3. Identifying application control requirements is not a step in a DRP, but rather a part of the application development and maintenance process that ensures the quality, security, and reliability of the software applications used by the organization.
Therefore, obtaining replacement supplies is the correct answer.
What is a Disaster Recovery Plan? + Complete Checklist
Risk Assessment - ISACA
Disaster Recovery Planning - ISACA
[Application Controls - ISACA]

QUESTION 2
Which of the following is the BEST indication that there are potential problems within an organization's IT service desk function?

A. Undocumented operating procedures
B. Lack of segregation of duties
C. An excessive backlog of user requests
D. Lack of key performance indicators (KPIs)

Correct Answer: C
Section:
Explanation:
An IT service desk is a function that provides technical support and assistance to the users of an organization's IT systems and services. An IT service desk typically handles issues such as software installation, hardware troubleshooting, network connectivity, password reset, system configuration, and user training. An IT service desk aims to ensure that the IT systems and services are available, reliable, secure, and efficient for the users.
One of the best indications that there are potential problems within an organization's IT service desk function is an excessive backlog of user requests. A backlog is a list of user requests that have not been resolved or completed by the IT service desk within a specified time frame. An excessive backlog means that the IT service desk is unable to meet the demand or expectations of the users, and that the users are experiencing delays, dissatisfaction, or frustration with the IT service desk.

An excessive backlog of user requests can indicate various problems within the IT service desk function, such as:
Insufficient staff, resources, or capacity to handle the volume or complexity of user requests
Ineffective processes, procedures, or tools for managing, prioritizing, or resolving user requests
Lack of skills, knowledge, or training among the IT service desk staff to deal with different types of user requests
Poor communication, collaboration, or coordination among the IT service desk staff or with other IT functions or stakeholders
Low quality, performance, or security of the IT systems or services that cause frequent or recurring user issues
Therefore, an excessive backlog of user requests is the best indication that there are potential problems within an organization's IT service desk function.
What is an IT Service Desk? Definition and Functions - Indeed
The Most Common IT Help Desk Issues - SherpaDesk
18 Common IT Help Desk Problems and Solutions - E-Pulse Blog

QUESTION 3
A source code repository should be designed to:

A. prevent changes from being incorporated into existing code.
B. prevent developers from accessing secure source code.
C. provide secure versioning and backup capabilities for existing code.
D. provide automatic incorporation and distribution of modified code.

Correct Answer: C
Section:
Explanation:
A source code repository is a system that stores and manages the source code of a software project. A source code repository should be designed to provide secure versioning and backup capabilities for existing code, as these are essential features for concurrent development, code quality, and disaster recovery. Versioning allows developers to track, compare, and revert changes to the code over time. Backup ensures that the code is safely stored and can be restored in case of data loss or corruption.
Reference
Source Code Repositories: What is a Source Code Repository?
Git Source Code Repository Design Considerations
Best practices for repositories - GitHub Docs

QUESTION 4
Which of the following would a digital signature MOST likely prevent?

A. Repudiation
B. Unauthorized change
C. Corruption
D. Disclosure

Correct Answer: B
Section:
Explanation:
A digital signature is a cryptographic technique that uses the sender's private key to generate a unique code for a message or document. The receiver can use the sender's public key to verify the authenticity and integrity of the message or document. A digital signature can prevent unauthorized change, as any modification to the message or document will invalidate the signature and alert the receiver of tampering.
Reference
What is a digital signature?
Digital Signature - an overview | ScienceDirect Topics
ISACA CISA Review Manual, 27th Edition, page 253

QUESTION 5

Which of the following should be an IS auditor's PRIMARY consideration when determining which issues to include in an audit report?

A. Professional skepticism
B. Management's agreement
C. Materiality
D. Inherent risk

Correct Answer: C
Section:
Explanation:
Materiality is the primary consideration when determining which issues to include in an audit report, as it reflects the significance or importance of the issues to the users of the report. Materiality is a relative concept that depends on the nature, context, and amount of the issues, as well as the expectations and needs of the users. Materiality helps the auditor to prioritize the issues and communicate them clearly and concisely.
Reference
ISACA CISA Review Manual, 27th Edition, page 256
Materiality in Auditing - AICPA
Materiality in Planning and Performing an Audit - IAASB

QUESTION 6
When designing a data analytics process, which of the following should be the stakeholder's role in automating data extraction and validation?

A. Indicating which data elements are necessary to make informed decisions
B. Allocating the resources necessary to purchase the appropriate software packages
C. Performing the business case analysis for the data analytics initiative
D. Designing the workflow necessary for the data analytics tool to evaluate the appropriate data

Correct Answer: A
Section:
Explanation:
The stakeholder's role in automating data extraction and validation is to indicate which data elements are necessary to make informed decisions. The stakeholder is the person who has a vested interest in the outcome of the data analytics process and can provide the business context and requirements for the analysis. The stakeholder can help the data analyst to identify the relevant data sources, the key performance indicators (KPIs), and the expected results of the analysis.
Reference
What Is the Data Analysis Process? 5 Key Steps to Follow - G2
What's the Best Approach to Data Analytics? - Harvard Business Review
Weekly challenge 1 - GitHub: Let's build from here

QUESTION 7
While evaluating the data classification process of an organization, an IS auditor's PRIMARY focus should be on whether:

A. data classifications are automated.
B. a data dictionary is maintained.
C. data retention requirements are clearly defined.
D. data is correctly classified.

Correct Answer: D
Section:
Explanation:
Data classification is the process of organizing and labeling data into categories based on file type, contents, and other metadata. Data classification helps organizations answer important questions about their data that

inform how they mitigate risk and manage data governance policies.Data classification also enables appropriate protection measures, and efficient search, retrieval and use of each data category12.
While evaluating the data classification process of an organization, an IS auditor's primary focus should be on whether data is correctly classified. This means that the data is assigned to the appropriate classification level based on its sensitivity, importance, integrity, availability, compliance requirements, and business value.Correct data classification ensures that the data is protected according to its risk level, and that the organization can comply with relevant laws and regulations that apply to different types of data3.
The other three options are not the primary focus of an IS auditor while evaluating the data classification process, although they may be relevant or useful for certain aspects of data management. Data classifications are automated means that the organization uses software tools or algorithms to analyze and label data based on predefined rules or criteria. This can improve the efficiency and consistency of data classification, but it does not guarantee that the data is correctly classified. The IS auditor still needs to verify the accuracy and validity of the automated classifications, and check for any errors or anomalies.
A data dictionary is maintained means that the organization keeps a record of the definitions, formats, sources, and relationships of the data elements in its systems or databases. This can enhance the understanding and usability of the data, but it does not ensure that the data is correctly classified. The IS auditor still needs to examine the content and context of the data, and compare it with the classification criteria and policies.
Data retention requirements are clearly defined means that the organization specifies how long it will keep different types of data, and when it will delete or archive them. This can help reduce storage costs, improve performance, and comply with legal obligations, but it does not ensure that the data is correctly classified. The IS auditor still needs to assess whether the data is stored and protected according to its classification level, and whether the retention periods are appropriate for each type of data.
Therefore, data is correctly classified is the best answer.
Data Classification: The Basics and a 6-Step Checklist - NetApp
What is Data Classification? Guidelines and Process - Varonis
Data Classification and Handling Procedures Guide

QUESTION 8
An IS auditor is preparing a plan for audits to be carried out over a specified period. Which of the following activities should the IS auditor perform FIRST?

A. Allocate audit resources.
B. Prioritize risks.
C. Review prior audit reports.
D. Determine the audit universe.

Correct Answer: D
Section:
Explanation:
An audit universe is a comprehensive list of all the auditable entities, processes, and activities within an organization. It helps the IS auditor to identify the scope, objectives, and priorities of the audit plan, as well as the resources and methodologies required to conduct the audits. An audit universe can also help the IS auditor to ensure that all the key risks, controls, and regulations are covered by the audit plan, and that there are no gaps or overlaps in the audit coverage.
The first activity that the IS auditor should perform when preparing a plan for audits to be carried out over a specified period is to determine the audit universe. This involves defining the criteria and methods for identifying and categorizing the auditable units, such as by business function, process, system, location, or risk level. The IS auditor should also consult with the management and other stakeholders to obtain their input and expectations for the audit plan. The IS auditor should then document and validate the audit universe, and update it regularly to reflect any changes in the organization's structure, operations, or environment.
The other three activities are also important for preparing an audit plan, but they should be performed after determining the audit universe. Allocating audit resources involves assigning staff, time, budget, and tools to each audit based on their complexity, priority, and availability. Prioritizing risks involves assessing the likelihood and impact of each risk associated with each auditable unit, and ranking them according to their significance and urgency. Reviewing prior audit reports involves analyzing the findings, recommendations, and actions from previous audits related to each auditable unit, and evaluating their current status and relevance.
Therefore, determining the audit universe is the best answer.
Audit Universe -- UPDATED 2022 -- Examples, Templates & More!
01 February 2023 Audit universe - IIA

QUESTION 9
When assessing the overall effectiveness of an organization's disaster recovery planning process, which of the following is MOST important for the IS auditor to verify?

A. Management contracts with a third party for warm site services.
B. Management schedules an annual tabletop exercise.
C. Management documents and distributes a copy of the plan to all personnel.
D. Management reviews and updates the plan annually or as changes occur.

Correct Answer: D
Section:
Explanation:
The overall effectiveness of an organization's disaster recovery planning process depends on how well the plan reflects the current and future needs and risks of the organization, and how well the plan is tested, communicated, and maintained. Among the four options given, the most important one for the IS auditor to verify is that management reviews and updates the plan annually or as changes occur.
A disaster recovery plan is not a static document that can be created once and forgotten. It is a dynamic and evolving process that requires regular review and update to ensure that it remains relevant, accurate, and effective. A disaster recovery plan should be reviewed and updated at least annually, or whenever there are significant changes in the organization's structure, operations, environment, or regulations. These changes could affect the business impact analysis, risk assessment, recovery objectives, recovery strategies, roles and responsibilities, or resources of the disaster recovery plan. If the plan is not updated to reflect these changes, it could become obsolete, incomplete, or inconsistent, and fail to meet the organization's recovery needs or expectations.
The other three options are not as important as reviewing and updating the plan, although they may also contribute to the effectiveness of the disaster recovery planning process. Contracting with a third party for warm site services is a possible recovery strategy that involves using a partially equipped facility that can be quickly activated in case of a disaster. However, this strategy may not be suitable or sufficient for every organization or scenario, and it does not guarantee the success of the disaster recovery plan. Scheduling an annual tabletop exercise is a good practice that involves simulating a disaster scenario and testing the plan in a hypothetical setting. However, this exercise may not be enough to evaluate the feasibility or readiness of the plan, and it should be complemented by other types of tests, such as walkthroughs, drills, or full-scale exercises. Documenting and distributing a copy of the plan to all personnel is an essential step that ensures that everyone involved in or affected by the plan is aware of their roles and responsibilities, and has access to the relevant information and instructions. However, this step alone does not ensure that the plan is understood or followed by all personnel, and it should be accompanied by proper training, education, and awareness programs.
Therefore, reviewing and updating the plan annually or as changes occur is the best answer.

QUESTION 10
In the development of a new financial application, the IS auditor's FIRST involvement should be in the:

A. control design.
B. feasibility study.
C. application design.
D. system test.

Correct Answer: B
Section:
Explanation:
In the development of a new financial application, the IS auditor's first involvement should be in the feasibility study. A feasibility study is a preliminary analysis that evaluates the technical, operational, economic, and legal aspects of a proposed project or system. A feasibility study helps determine whether the project or system is viable, feasible, and desirable for the organization and its stakeholders.
The IS auditor's role in the feasibility study is to provide an independent and objective assessment of the project or system's risks, benefits, costs, and impacts. The IS auditor should also ensure that the feasibility study follows a structured and systematic approach, considers all relevant factors and alternatives, and complies with the organization's policies and standards. The IS auditor should also verify that the feasibility study is documented and communicated to the appropriate decision-makers.
The IS auditor's involvement in the feasibility study is important because it can help:
Identify and mitigate potential risks and issues that could affect the project or system's success
Evaluate and justify the project or system's alignment with the organization's strategy, goals, and value proposition
Estimate and optimize the project or system's resources, budget, schedule, and quality
Assess and enhance the project or system's security, reliability, performance, and usability
Ensure that the project or system meets the expectations and requirements of the users and other stakeholders
The other three options are not the first involvement of the IS auditor in the development of a new financial application, although they may be part of the subsequent stages of the development process. Control design is the process of defining and implementing controls that ensure the security, integrity, availability, and efficiency of the system. Application design is the process of specifying the functional and technical features of the system. System test is the process of verifying that the system meets the specifications and requirements.
Therefore, feasibility study is the best answer.
[Feasibility Study - ISACA]
[IS Auditing Guideline G13 Performing an IS Audit Engagement - ISACA]

QUESTION 11
An IS auditor finds that the process for removing access for terminated employees is not documented What is the MOST significant risk from this observation?

A. Procedures may not align with best practices
B. Human resources (HR) records may not match system access.
C. Unauthorized access cannot he identified.
D. Access rights may not be removed in a timely manner.

Correct Answer: D
Section:
Explanation:
The most significant risk from this observation is that access rights may not be removed in a timely manner. If the process for removing access for terminated employees is not documented, there is no clear guidance or accountability for who, how, when, and what actions should be taken to revoke the access rights of the employees who leave the organization. This could result in delays, inconsistencies, or omissions in removing access rights, which could allow terminated employees to retain unauthorized access to the organization's systems and data. This could compromise the security, confidentiality, integrity, and availability of the information assets.Reference:
CISA Review Manual (Digital Version)
CISA Questions, Answers & Explanations Database

QUESTION 12
The PRIMARY objective of value delivery in reference to IT governance is to:

A. promote best practices
B. increase efficiency.
C. optimize investments.
D. ensure compliance.

Correct Answer: C
Section:
Explanation:
The primary objective of value delivery in reference to IT governance is to optimize investments. Value delivery is one of the five focus areas of IT governance that aims to ensure that IT delivers expected benefits to stakeholders and enables business value creation. Value delivery involves aligning IT investments with business objectives and strategies, managing IT performance and benefits realization, optimizing IT costs and risks, and enhancing IT innovation and agility. Value delivery helps to maximize the return on investment (ROI) and value for money (VFM) of IT resources and capabilities.Reference:
CISA Review Manual (Digital Version)
CISA Questions, Answers & Explanations Database

QUESTION 13
What should an IS auditor do FIRST upon discovering that a service provider did not notify its customers of a security breach?

A. Notify law enforcement of the finding.
B. Require the third party to notify customers.
C. The audit report with a significant finding.
D. Notify audit management of the finding.

Correct Answer: D
Section:
Explanation:
The IS auditor should notify audit management of the finding first, as this is a significant issue that may affect the audit scope and objectives. The IS auditor should not notify law enforcement or require the third party to notify customers without consulting audit management first. The audit report with a significant finding should be issued after the audit is completed and the findings are validated.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 247

QUESTION 14

Which of the following is a challenge in developing a service level agreement (SLA) for network services?

A. Establishing a well-designed framework for network servirces.
B. Finding performance metrics that can be measured properly
C. Ensuring that network components are not modified by the client
D. Reducing the number of entry points into the network

Correct Answer: B
Section:
Explanation:
One of the challenges in developing a SLA for network services is finding performance metrics that can be measured properly and reflect the quality of service expected by the customer. Establishing a well-designed framework for network services is not a challenge, but a good practice. Ensuring that network components are not modified by the client or reducing the number of entry points into the network are security issues, not SLA issues.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 333

QUESTION 15
A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

A. Using smart cards with one-time passwords
B. Periodically reviewing log files
C. Configuring the router as a firewall
D. Installing biometrics-based authentication

Correct Answer: B
Section:
Explanation:
Periodically reviewing log files is the most effective way to detect intrusion attempts from outside the organization, as they can provide evidence of unauthorized access attempts, source IP addresses, timestamps and other relevant information. Using smart cards with one-time passwords or installing biometrics-based authentication can prevent unauthorized access, but not detect it. Configuring the router as a firewall can block unwanted traffic, but not log it.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 361

QUESTION 16
An organization has virtualized its server environment without making any other changes to the network or security infrastructure. Which of the following is the MOST significant risk?

A. Inability of the network intrusion detection system (IDS) to monitor virtual server-lo-server communications
B. Vulnerability in the virtualization platform affecting multiple hosts
C. Data center environmental controls not aligning with new configuration
D. System documentation not being updated to reflect changes in the environment

Correct Answer: A
Section:
Explanation:
The most significant risk in virtualizing the server environment without making any other changes to the network or security infrastructure is the inability of the network intrusion detection system (IDS) to monitor virtual server-to-server communications. This can create blind spots for the IDS and allow malicious traffic to bypass detection. A vulnerability in the virtualization platform affecting multiple hosts is a potential risk, but not necessarily more significant than the loss of visibility. Data center environmental controls not aligning with new configuration or system documentation not being updated to reflect changes in the environment are operational issues, not security issues.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 373

QUESTION 17
Which of the following should be of GREATEST concern to an IS auditor reviewing a network printer disposal process?

A. Disposal policies and procedures are not consistently implemented
B. Evidence is not available to verify printer hard drives have been sanitized prior to disposal.
C. Business units are allowed to dispose printers directly to
D. Inoperable printers are stored in an unsecured area.

Correct Answer: B
Section:
Explanation:
The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 387

QUESTION 18
Which of the following backup schemes is the BEST option when storage media is limited?

A. Real-time backup
B. Virtual backup
C. Differential backup
D. Full backup

Correct Answer: C
Section:
Explanation:
A differential backup scheme is the best option when storage media is limited, as it only backs up the data that has changed since the last full backup. This reduces the amount of storage space required and also simplifies the restoration process, as only the last full backup and the last differential backup are needed. A real-time backup scheme would require continuous replication of data, which would consume a lot of storage space and network bandwidth. A virtual backup scheme would create a snapshot of the data at a point in time, but it would not reduce the storage space required, as it would still need to store the changes made to the data. A full backup scheme would back up all the data every time, which would require the most storage space and also take longer to complete.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 405

QUESTION 19
During an IT general controls audit of a high-risk area where both internal and external audit teams are reviewing the same approach to optimize resources?

A. Leverage the work performed by external audit for the internal audit testing.
B. Ensure both the internal and external auditors perform the work simultaneously.
C. Request that the external audit team leverage the internal audit work.
D. Roll forward the general controls audit to the subsequent audit year.

Correct Answer: A
Section:
Explanation:
The best approach to optimize resources when both internal and external audit teams are reviewing the same IT general controls area is to leverage the work performed by external audit for the internal audit testing. This can avoid duplication of efforts, reduce audit costs and enhance coordination between the audit teams. The internal audit team should evaluate the quality and reliability of the external audit work before relying on it. Ensuring both the internal and external auditors perform the work simultaneously is not an efficient use of resources, as it would create redundancy and possible interference. Requesting that the external audit team leverage the internal audit work may not be feasible or acceptable, as the external audit team may have different objectives, standards and independence requirements. Rolling forward the general controls audit to the subsequent audit year is not a good practice, as it would delay the identification and remediation of any control weaknesses in a high-risk area.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 247

QUESTION 20
Which of the following is a corrective control?

A. Separating equipment development testing and production
B. Verifying duplicate calculations in data processing
C. Reviewing user access rights for segregation
D. Executing emergency response plans

Correct Answer: D
Section:
Explanation:
A corrective control is a control that aims to restore normal operations after a disruption or incident has occurred. Executing emergency response plans is an example of a corrective control, as it helps to mitigate the impact of an incident and resume business functions. Separating equipment development testing and production is a preventive control, as it helps to avoid errors or unauthorized changes in production systems. Verifying duplicate calculations in data processing is a detective control, as it helps to identify errors or anomalies in data processing. Reviewing user access rights for segregation is also a detective control, as it helps to detect any violations of segregation of duties principles.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 64

QUESTION 21
An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business The auditor's PRIMARY concern would be:

A. failure to maximize the use of equipment
B. unanticipated increase in business s capacity needs.
C. cost of excessive data center storage capacity
D. impact to future business project funding.

Correct Answer: B
Section:
Explanation:
The auditor's primary concern when capacity management for a key system is being performed by IT with no input from the business would be an unanticipated increase in business's capacity needs. This could result in performance degradation, service disruption or customer dissatisfaction if IT is not able to provide sufficient capacity to meet the business demand. Failure to maximize the use of equipment, cost of excessive data center storage capacity or impact to future business project funding are secondary concerns that relate to resource optimization or budget allocation, but not to service delivery or customer satisfaction.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 374

QUESTION 22
Which of the following IT service management activities is MOST likely to help with identifying the root cause of repeated instances of network latency?

A. Change management
B. Problem management
C. incident management
D. Configuration management

Correct Answer: B
Section:
Explanation:
Problem management is an IT service management activity that is most likely to help with identifying the root cause of repeated instances of network latency. Problem management involves analyzing incidents that affect IT services and finding solutions to prevent them from recurring or minimize their impact. Change management is an IT service management activity that involves controlling and documenting any modifications to IT services or infrastructure. Incident management is an IT service management activity that involves restoring normal service operation as quickly as possible after an incident has occurred. Configuration management is an IT service management activity that involves identifying and maintaining records of IT assets and their relationships.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 334

QUESTION 23
The PRIMARY benefit of information asset classification is that it:

A. prevents loss of assets.
B. helps to align organizational objectives.
C. facilitates budgeting accuracy.
D. enables risk management decisions.

Correct Answer: D
Section:
Explanation:
The primary benefit of information asset classification is that it enables risk management decisions. Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 300

QUESTION 24
Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?

A. Program coding standards have been followed
B. Acceptance test criteria have been developed
C. Data conversion procedures have been established.
D. The design has been approved by senior management.

Correct Answer: B
Section:
Explanation:
The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase. Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 323

QUESTION 25
Which of the following should be the IS auditor's PRIMARY focus, when evaluating an organization's offsite storage facility?

A. Shared facilities
B. Adequacy of physical and environmental controls
C. Results of business continuity plan (BCP) test
D. Retention policy and period

Correct Answer: B
Section:
Explanation:
The IS auditor's primary focus when evaluating an organization's offsite storage facility should be the adequacy of physical and environmental controls. Physical and environmental controls are essential to protect the offsite storage facility from unauthorized access, theft, fire, water damage, pests or other hazards that could compromise the integrity and availability of backup media. Shared facilities is something that the IS auditor should consider when evaluating the offsite storage facility, but it is not the primary focus. Results of business continuity plan (BCP) test or retention policy and period are things that the IS auditor should review when evaluating the organization's BCP or backup strategy, not the offsite storage facility itself.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 388

QUESTION 26
Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's disaster recovery plan (DRP)?

A. The DRP has not been formally approved by senior management.
B. The DRP has not been distributed to end users.
C. The DRP has not been updated since an IT infrastructure upgrade.
D. The DRP contains recovery procedures for critical servers only.

Correct Answer: C
Section:
Explanation:
The greatest concern for an IS auditor reviewing an organization's disaster recovery plan (DRP) is that the DRP has not been updated since an IT infrastructure upgrade. This could render the DRP obsolete or ineffective, as it may not reflect the current configuration, dependencies or recovery requirements of the IT systems. The IS auditor should ensure that the DRP is reviewed and updated regularly to align with any changes in the IT environment. The DRP has not been formally approved by senior management is a concern for an IS auditor reviewing an organization's DRP, but it is not as critical as ensuring that the DRP is up to date and valid. The DRP has not been distributed to end users or the DRP contains recovery procedures for critical servers only are issues that relate to the communication or scope of the DRP, but not to its validity or effectiveness.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 389

QUESTION 27
Which of the following is MOST critical for the effective implementation of IT governance?

A. Strong risk management practices
B. Internal auditor commitment
C. Supportive corporate culture
D. Documented policies

Correct Answer: C
Section:
Explanation:
The most critical factor for the effective implementation of IT governance is a supportive corporate culture. A supportive corporate culture is one that fosters collaboration, communication and commitment among all stakeholders involved in IT governance processes. A supportive corporate culture also promotes a shared vision, values and goals for IT governance across the organization. Strong risk management practices, internal auditor commitment or documented policies are important elements for IT governance implementation, but they are not sufficient without a supportive corporate culture.Reference:ISACA, CISA Review Manual, 27th Edition, 2018, page 41

QUESTION 28
Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

A. Inability to utilize the site when required
B. Inability to test the recovery plans onsite
C. Equipment compatibility issues at the site
D. Mismatched organizational security policies

Correct Answer: A
Section:
Explanation:
The greatest risk of using a reciprocal site for disaster recovery is the inability to utilize the site when required. A reciprocal site is an agreement between two organizations to provide backup facilities for each other in case of a disaster. However, this arrangement may not be reliable or enforceable, especially if both organizations are affected by the same disaster or have conflicting priorities.Therefore, the IS auditor should recommend that management consider alternative options for disaster recovery, such as dedicated sites or cloud services12.Reference:
CISA Review Manual, 27th Edition, page 3381
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 29
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

A. Risk avoidance
B. Risk transfer
C. Risk acceptance
D. Risk reduction

Correct Answer: A
Section:
Explanation:
The approach adopted by management in this scenario is risk avoidance.Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a threat to the organization3. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case.Reference:
CISA Review Manual, 27th Edition, page 641
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 30
Which of the following is the BEST control lo mitigate attacks that redirect Internet traffic to an unauthorized website?

A. Utilize a network-based firewall.
B. Conduct regular user security awareness training.
C. Perform domain name system (DNS) server security hardening.
D. Enforce a strong password policy meeting complexity requirement.

Correct Answer: C
Section:
Explanation:
The best control to mitigate attacks that redirect Internet traffic to an unauthorized website is to perform domain name system (DNS) server security hardening.DNS servers are responsible for resolving domain names into IP addresses, and they are often targeted by attackers who want to manipulate or spoof DNS records to redirect users to malicious websites4. By applying security best practices to DNS servers, such as encrypting DNS traffic, implementing DNSSEC, restricting access and updating patches, the organization can reduce the risk of DNS hijacking attacks. A network-based firewall, user security awareness training and a strong password policy are also important controls, but they are not as effective as DNS server security hardening in preventing this specific type of attack.Reference:
CISA Review Manual, 27th Edition, page 4021
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 31
An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported the auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

A. Verify all patches have been applied to the software system's outdated version
B. Close all unused ports on the outdated software system.
C. Segregate the outdated software system from the main network.
D. Monitor network traffic attempting to reach the outdated software system.

Correct Answer: C
Section:
Explanation:

The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. An unsupported software system may have unpatched vulnerabilities that could be exploited by attackers to compromise the system or access sensitive data. By isolating the system from the rest of the network, the organization can limit the exposure and impact of a potential breach. Verifying all patches have been applied to the outdated software system, closing all unused ports on the outdated software system and monitoring network traffic attempting to reach the outdated software system are also good practices, but they do not address the root cause of the risk, which is the lack of vendor support and updates.Reference:
CISA Review Manual, 27th Edition, page 2951
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 32
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Apply single sign-on for access control
B. Implement segregation of duties.
C. Enforce an internal data access policy.
D. Enforce the use of digital signatures.

Correct Answer: C
Section:
Explanation:
The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential information from the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy.Reference:
CISA Review Manual, 27th Edition, page 2301
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

QUESTION 33
Which of the following would be MOST effective to protect information assets in a data center from theft by a vendor?

A. Monitor and restrict vendor activities
B. Issues an access card to the vendor.
C. Conceal data devices and information labels
D. Restrict use of portable and wireless devices.

Correct Answer: A
Section:
Explanation:
The most effective control to protect information assets in a data center from theft by a vendor is to monitor and restrict vendor activities. A vendor may have legitimate access to the data center for maintenance or support purposes, but they may also have malicious intentions or be compromised by an attacker. By monitoring and restricting vendor activities, the organization can ensure that the vendor only performs authorized tasks and does not access or tamper with sensitive data or equipment. Issuing an access card to the vendor, concealing data devices and information labels, and restricting use of portable and wireless devices are also useful controls, but they are not as effective as monitoring and restricting vendor activities in preventing theft by a vendor.Reference:
CISA Review Manual, 27th Edition, page 3381
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 34
An IS auditor discovers that an IT organization serving several business units assigns equal priority to all initiatives, creating a risk of delays in securing project funding Which of the following would be MOST helpful in matching demand for projects and services with available resources in a way that supports business objectives?

A. Project management
B. Risk assessment results
C. IT governance framework
D. Portfolio management

Correct Answer: D
Section:
Explanation:
The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management.Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and services with the strategic goals and value proposition of the organization3. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services.Reference:
CISA Review Manual, 27th Edition, page 721
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 35
An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

A. Loss of application support
B. Lack of system integrity
C. Outdated system documentation
D. Developer access 1o production

Correct Answer: B
Section:
Explanation:
The most significant risk from not testing patches before putting them into production is the lack of system integrity. Patches are software updates that fix bugs, vulnerabilities or performance issues in an application system.However, patches may also introduce new errors, conflicts or compatibility issues that could affect the functionality, reliability or security of the system4. By not testing patches before putting them into production, the organization exposes itself to the risk of system failures, data corruption or unauthorized access. Loss of application support, outdated system documentation and developer access to production are also risks from not testing patches, but they are not as significant as the lack of system integrity.Reference:
CISA Review Manual, 27th Edition, page 2951
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 36
What is the PRIMARY purpose of documenting audit objectives when preparing for an engagement?

A. To address the overall risk associated with the activity under review
B. To identify areas with relatively high probability of material problems
C. To help ensure maximum use of audit resources during the engagement
D. To help prioritize and schedule auditee meetings

Correct Answer: B
Section:
Explanation:
The primary purpose of documenting audit objectives when preparing for an engagement is to identify areas with relatively high probability of material problems. Audit objectives are statements that describe what the audit intends to accomplish or verify during the engagement. Audit objectives help the IS auditor to focus on the key areas of risk or concern, to design appropriate audit procedures and tests, and to evaluate audit evidence and results. By documenting audit objectives, the IS auditor can identify areas with relatively high probability of material problems that may affect the achievement of audit goals or business objectives. Addressing the overall risk

associated with the activity under review, ensuring maximum use of audit resources during the engagement and prioritizing and scheduling auditee meetings are also purposes of documenting audit objectives, but they are not as primary as identifying areas with high probability of material problems.Reference:
CISA Review Manual, 27th Edition, page 1111
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 37
Which of the following should be the FIRST step in the incident response process for a suspected breach?

A. Inform potentially affected customers of the security breach
B. Notify business management of the security breach.
C. Research the validity of the alerted breach
D. Engage a third party to independently evaluate the alerted breach.

Correct Answer: C
Section:
Explanation:
The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the incident response process, but they are not the first step.Reference:
CISA Review Manual, 27th Edition, page 4251
CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 38
An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be MOST useful to the auditor?

A. Manual sign-in and sign-out log
B. System electronic log
C. Alarm system with CCTV
D. Security incident log

Correct Answer: B
Section:
Explanation:
A system electronic log is the most useful source of information for an IS auditor to review all access attempts to a video-monitored and proximity card-controlled communications room. A system electronic log can provide accurate and detailed records of the date, time, card number, and status (success or failure) of each access attempt. A system electronic log can also be easily searched, filtered, and analyzed by the auditor to identify any unauthorized or suspicious access attempts.
A manual sign-in and sign-out log is not as reliable or useful as a system electronic log, because it depends on the honesty and compliance of the users. A manual log can be easily manipulated, forged, or omitted by the users or intruders. A manual log also does not capture the status of each access attempt, and it can be difficult to verify the identity of the users based on their signatures.
An alarm system with CCTV is not as useful as a system electronic log, because it only captures the events that trigger the alarm, such as unauthorized or forced entry. An alarm system with CCTV does not provide a complete record of all access attempts, and it can be affected by factors such as camera angle, lighting, and resolution. An alarm system with CCTV also requires more time and effort to review the video footage by the auditor.
A security incident log is not as useful as a system electronic log, because it only records the incidents that are reported by the users or detected by the security staff. A security incident log does not provide a comprehensive record of all access attempts, and it can be incomplete or inaccurate depending on the reporting and detection mechanisms. A security incident log also does not capture the details of each access attempt, such as the card number and status.
ISACA CISA Review Manual 27th Edition (2019), page 247
ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB

QUESTION 39
Which of the following should be the FRST step when developing a data toes prevention (DIP) solution for a large organization?

A. Identify approved data workflows across the enterprise.
B. Conduct a threat analysis against sensitive data usage.
C. Create the DLP pcJc.es and templates
D. Conduct a data inventory and classification exercise

Correct Answer: D
Section:
Explanation:
The first step when developing a data loss prevention (DLP) solution for a large organization is to conduct a data inventory and classification exercise. This step is essential to identify the types, locations, owners, and sensitivity levels of the data that need to be protected by the DLP solution. A data inventory and classification exercise helps to define the scope, objectives, and requirements of the DLP solution, as well as to prioritize the data protection efforts based on the business value and risk of the data. A data inventory and classification exercise also enables the organization to comply with relevant laws and regulations regarding data privacy and security.
The other options are not the first step when developing a DLP solution, but rather subsequent steps that depend on the outcome of the data inventory and classification exercise. Identifying approved data workflows across the enterprise is a step that helps to design and implement the DLP policies and controls that match the business processes and data flows. Conducting a threat analysis against sensitive data usage is a step that helps to assess and mitigate the risks associated with data leakage, theft, or misuse. Creating the DLP policies and templates is a step that helps to enforce the data protection rules and standards across the organization.
ISACA CISA Review Manual 27th Edition (2019), page 247
Data Loss Prevention---Next Steps - ISACA1
What is data loss prevention (DLP)?| Microsoft Security

QUESTION 40
An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

A. Abuses by employees have not been reported.
B. Lessons learned have not been properly documented
C. vulnerabilities have not been properly addressed
D. Security incident policies are out of date.

Correct Answer: C
Section:
Explanation:
The major concern with the situation where security incidents are resolved and closed, but root causes are not investigated, is that vulnerabilities have not been properly addressed. Vulnerabilities are weaknesses or gaps in the security posture of an organization that can be exploited by threat actors to compromise its systems, data, or operations. If root causes are not investigated, vulnerabilities may remain undetected or unresolved, allowing attackers to exploit them again or use them as entry points for further attacks. This can result in repeated or escalated security incidents that can cause more damage or disruption to the organization.
The other options are not as major as the concern about vulnerabilities, but rather secondary or related issues that may arise from the lack of root cause analysis. Abuses by employees have not been reported is a concern that may indicate a lack of awareness, accountability, or monitoring of insider threats. Lessons learned have not been properly documented is a concern that may indicate a lack of improvement, learning, or feedback from security incidents. Security incident policies are out of date is a concern that may indicate a lack of alignment, review, or update of security incident processes.
ISACA CISA Review Manual 27th Edition (2019), page 254
Why Root Cause Analysis is Crucial to Incident Response (IR) - Avertium3
Root Cause Analysis Steps and How it Helps Incident Response ...

QUESTION 41
Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

A. Review of program documentation
B. Use of test transactions
C. Interviews with knowledgeable users
D. Review of source code

Correct Answer: B
Section:
Explanation:
The most conclusive audit procedure for evaluating the effectiveness of an e-commerce application system's edit routine is to use test transactions.A test transaction is a simulated input that is processed by the system to verify its output and performance1. By using test transactions, an auditor can directly observe how the edit routine checks the validity, accuracy, and completeness of data entered by users, and how it handles incorrect or invalid data. A test transaction can also help measure the efficiency, reliability, and security of the edit routine, as well as identify any errors or weaknesses in the system.
The other options are not as conclusive as using test transactions, as they rely on indirect or secondary sources of information.Reviewing program documentation is an audit procedure that involves examining the written description of the system's design, specifications, and functionality2. However, program documentation may not reflect the actual implementation or operation of the system, and it may not reveal any discrepancies or defects in the edit routine.Interviews with knowledgeable users is an audit procedure that involves asking questions to the people who use or manage the system3. However, interviews with knowledgeable users may not provide sufficient or objective evidence of the edit routine's effectiveness, and they may be influenced by personal opinions or biases.Reviewing source code is an audit procedure that involves analyzing the programming language and logic of the system4. However, reviewing source code may not be feasible or practical for complex or large systems, and it may not demonstrate how the edit routine performs in real scenarios.

QUESTION 42
A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

A. A formal request for proposal (RFP) process
B. Business case development procedures
C. An information asset acquisition policy
D. Asset life cycle management.

Correct Answer: D
Section:
Explanation:
Asset life cycle management is a technique of asset management where facility managers maximize the usable life of assets through planning, purchasing, using, maintaining, and disposing of assets1.The main aim of asset life cycle management is to reduce costs and increase productivity by optimizing the performance, reliability, and lifespan of assets2.Asset life cycle management can help prevent the situation of having unused applications by ensuring that the applications are aligned with the business needs, objectives, and strategies, and that they are regularly reviewed, updated, or retired as necessary3.
The other options are not as effective as asset life cycle management for preventing unused applications. A formal request for proposal (RFP) process is a method of soliciting bids from potential vendors or suppliers for a project or service. A RFP process can help select the best application for a specific requirement, but it does not ensure that the application will be used or maintained throughout its lifecycle. Business case development procedures are a set of steps that involve defining the problem, analyzing the alternatives, and proposing a solution for a project or initiative. Business case development procedures can help justify the need and value of an application, but they do not guarantee that the application will be utilized or supported after its implementation. An information asset acquisition policy is a document that outlines the rules and standards for acquiring information assets such as applications. An information asset acquisition policy can help ensure that the applications are acquired in a consistent and compliant manner, but it does not address how the applications will be managed or disposed of after their acquisition.

QUESTION 43
An IS auditor follows up on a recent security incident and finds the incident response was not adequate. Which of the following findings should be considered MOST critical?

A. The security weakness facilitating the attack was not identified.
B. The attack was not automatically blocked by the intrusion detection system (IDS).
C. The attack could not be traced back to the originating person.
D. Appropriate response documentation was not maintained.

Correct Answer: A
Section:
Explanation:
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.
The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the

originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
ISACA CISA Review Manual 27th Edition (2019), page 254
Incident Response Process - ISACA1
Incident Response: How to Identify and Fix Security Weaknesses

QUESTION 44
in a controlled application development environment, the MOST important segregation of duties should be between the person who implements changes into the production environment and the:

A. application programmer
B. systems programmer
C. computer operator
D. quality assurance (QA) personnel

Correct Answer: A
Section:
Explanation:
In a controlled application development environment, the most important segregation of duties should be between the person who implements changes into the production environment and the application programmer. This segregation of duties ensures that no one person can create and deploy code without proper review, testing, and approval. This reduces the risk of errors, fraud, or malicious code being introduced into the production environment.
The other options are not as important as the segregation between the application programmer and the person who implements changes into production, but they are still relevant for achieving a secure and reliable application development environment. The segregation of duties between the person who implements changes into production and the systems programmer is important to prevent unauthorized or untested changes to system software or configuration. The segregation of duties between the person who implements changes into production and the computer operator is important to prevent unauthorized or uncontrolled access to production data or resources. The segregation of duties between the person who implements changes into production and the quality assurance (QA) personnel is important to ensure independent verification and validation of code quality and functionality.
ISACA CISA Review Manual 27th Edition (2019), page 247
Segregation of Duties in an Agile Environment | AKF Partners3
Separation of Duties: How to Conform in a DevOps World4

QUESTION 45
A review of Internet security disclosed that users have individual user accounts with Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only the corporate network is used. The organization should FIRST:

A. use a proxy server to filter out Internet sites that should not be accessed.
B. keep a manual log of Internet access.
C. monitor remote access activities.
D. include a statement in its security policy about Internet use.

Correct Answer: D
Section:
Explanation:
The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use.A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data1. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personal accounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.
The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.

ISACA CISA Review Manual 27th Edition (2019), page 247
What is a Security Policy?Definition, Elements, and Examples - Varonis1

QUESTION 46
Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

A. Customer service complaints
B. Automated monitoring of logs
C. Server crashes
D. Penetration testing

Correct Answer: B
Section:
Explanation:
The best way to detect that a distributed denial of service (DDoS) attack is occurring is to use automated monitoring of logs.A DDoS attack disrupts the operations of a server, service, or network by flooding it with unwanted Internet traffic2.Automated monitoring of logs can help pinpoint potential DDoS attacks by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and alerting administrators or security teams of any anomalies or malicious requests, protocols, or IP blocks3. Automated monitoring of logs can also help identify the source, type, and impact of the DDoS attack, and provide evidence for further investigation or mitigation.
The other options are not as effective as automated monitoring of logs for detecting DDoS attacks. Customer service complaints are an indirect and delayed indicator of a DDoS attack, as they rely on users reporting problems with accessing a website or service. Customer service complaints may also be caused by other factors unrelated to DDoS attacks, such as server errors or network issues. Server crashes are an extreme and undesirable indicator of a DDoS attack, as they indicate that the server has already been overwhelmed by the attack and has stopped functioning. Server crashes may also result in data loss or corruption, service disruption, or reputational damage. Penetration testing is a proactive and preventive measure for assessing the security posture of a system or network, but it does not detect ongoing DDoS attacks. Penetration testing may involve simulating DDoS attacks to test the resilience or vulnerability of a system or network, but it does not monitor real-time traffic or identify actual attackers.
ISACA CISA Review Manual 27th Edition (2019), page 254
How to prevent DDoS attacks | Methods and tools | Cloudflare2
Understanding Denial-of-Service Attacks | CISA3

QUESTION 47
Which of the following is MOST important when implementing a data classification program?

A. Understanding the data classification levels
B. Formalizing data ownership
C. Developing a privacy policy
D. Planning for secure storage capacity

Correct Answer: B
Section:
Explanation:
Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.
To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.
The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.
ISACA, CISA Review Manual, 27th Edition, 2020, page 247
Data Classification: What It Is and How to Implement It

QUESTION 48

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

A. Restricting program functionality according to user security profiles
B. Restricting access to update programs to accounts payable staff only
C. Including the creator's user ID as a field in every transaction record created
D. Ensuring that audit trails exist for transactions

Correct Answer: D
Section:
Explanation:
Segregation of duties (SoD) is a key internal control that aims to prevent fraud and errors by ensuring that no single individual can perform incompatible or conflicting tasks within a business process. SoD reduces the risk of unauthorized or improper transactions, manipulation of data, or misappropriation of assets.
In the accounts payable department, SoD involves separating the following functions: invoice processing, payment authorization, payment execution, and reconciliation. For example, the person who approves an invoice should not be the same person who issues the payment or reconciles the bank statement.
One of the best ways to ensure appropriate SoD within the accounts payable department is to restrict program functionality according to user security profiles. This means that each user of the accounts payable system should have a unique login and password, and should only have access to the functions that are relevant to their role and responsibilities. For instance, an invoice processor should not be able to approve payments or modify vendor records. This way, the system can enforce SoD and prevent unauthorized or fraudulent activities.
The other options are not as effective as restricting program functionality according to user security profiles. Restricting access to update programs to accounts payable staff only is a general access control measure, but it does not address the SoD issue within the accounts payable department. Including the creator's user ID as a field in every transaction record created is a useful audit trail feature, but it does not prevent users from performing incompatible functions. Ensuring that audit trails exist for transactions is a detective control that can help identify and investigate any irregularities, but it does not prevent them from occurring in the first place.

QUESTION 49
Which of the following would be MOST useful when analyzing computer performance?

A. Statistical metrics measuring capacity utilization
B. Operations report of user dissatisfaction with response time
C. Tuning of system software to optimize resource usage
D. Report of off-peak utilization and response time

Correct Answer: A
Section:
Explanation:
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
What is Computer Performance?
How to Measure Computer Performance

QUESTION 50
Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

A. Temperature sensors
B. Humidity sensors
C. Water sensors

D. Air pressure sensors

Correct Answer: C
Section:
Explanation:
Water sensors are devices that can detect the presence of water or moisture in a given area. They are often deployed below the floor tiles of a data center to monitor for any water leaks that may damage the equipment or cause electrical hazards. Water sensors can alert the data center staff or trigger an automatic response to prevent or mitigate the water leakage.
The other options are not likely to be deployed below the floor tiles of a data center. Temperature sensors and humidity sensors are usually deployed above the floor tiles to measure the ambient conditions of the data center and ensure optimal cooling and ventilation. Air pressure sensors are typically deployed at the air vents or ducts to monitor the airflow and pressure distribution in the data center.
Data Center Environmental Monitoring
Water Detection in Data Centers

QUESTION 51
Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

A. Ensure that paper documents arc disposed security.
B. Implement an intrusion detection system (IDS).
C. Verify that application logs capture any changes made.
D. Validate that all data files contain digital watermarks

Correct Answer: D
Section:
Explanation:
Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data leakage by deterring potential leakers from sharing sensitive data or by providing evidence of data leakage if it occurs.
The other options are not as effective as digital watermarks in preventing data leakage. Ensuring that paper documents are disposed securely can reduce the risk of physical data leakage, but it does not address the digital data leakage that is more prevalent in today's environment. Implementing an intrusion detection system (IDS) can help detect and respond to cyberattacks that may cause data leakage, but it does not prevent data leakage from insiders or authorized users who have legitimate access to the data. Verifying that application logs capture any changes made can help audit and investigate data leakage incidents, but it does not prevent them from happening in the first place.
What is Data Leakage?
What is Digital Watermarking?

QUESTION 52
An IS auditor assessing the controls within a newly implemented call center would First

A. gather information from the customers regarding response times and quality of service.
B. review the manual and automated controls in the call center.
C. test the technical infrastructure at the call center.
D. evaluate the operational risk associated with the call center.

Correct Answer: D
Section:
Explanation:
The first step in assessing the controls within a newly implemented call center is to evaluate the operational risk associated with the call center. This will help the IS auditor to identify the potential threats, vulnerabilities, and impacts that could affect the call center's objectives, performance, and availability. The evaluation of operational risk will also provide a basis for determining the scope, objectives, and approach of the audit. The other options are possible audit procedures, but they are not the first step in the audit process.Reference:ISACA Frameworks: Blueprints for Success,CISA Review Manual (Digital Version)

QUESTION 53
An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which

of two following is the MOST reliable follow-up procedure?

A. Review the documentation of recant changes to implement sequential order numbering.
B. Inquire with management if the system has been configured and tested to generate sequential order numbers.
C. Inspect the system settings and transaction logs to determine if sequential order numbers are generated.
D. Examine a sample of system generated purchase orders obtained from management

Correct Answer: C
Section:
Explanation:
The most reliable follow-up procedure to determine if management has resolved the finding of non-sequential purchase order numbers is to inspect the system settings and transaction logs to determine if sequential order numbers are generated. This will provide direct evidence of the system's functionality and compliance with the audit recommendation. The other options are less reliable because they rely on indirect evidence or information obtained from management, which may not be accurate or complete.Reference:CISA Review Manual (Digital Version),Standards, Guidelines, Tools and Techniques

QUESTION 54
When reviewing a data classification scheme, it is MOST important for an IS auditor to determine if.

A. each information asset is to a assigned to a different classification.
B. the security criteria are clearly documented for each classification
C. Senior IT managers are identified as information owner.
D. the information owner is required to approve access to the asset

Correct Answer: B
Section:
Explanation:
When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements.The security criteria should define the level of confidentiality, integrity, and availability for each data classification, as well as the corresponding controls such as access control, rights management, and cryptographic protection1. The other options are less important or incorrect because:
A . Each information asset is not necessarily assigned to a different classification.Data classification schemes usually have a limited number of categories, such as ''Sensitive,'' ''Confidential,'' and ''Public,'' and multiple information assets can belong to the same category2.
C . Senior IT managers are not necessarily identified as information owners.Information owners are typically the business units or functions that create, use, or maintain the information assets, and they may or may not be senior IT managers3.
D . The information owner is not required to approve access to the asset.The information owner is responsible for defining the access requirements and rules for the asset, but the actual approval of access requests may be delegated to other roles, such as data custodians or administrators3.Reference:Simplify and Contextualize Your Data Classification Efforts - ISACA,3.7: Establish and Maintain a Data Classification Scheme,Data Classification and Practices - NIST,CISA Exam Content Outline | CISA Certification | ISACA

QUESTION 55
Which of the following would be the MOST useful metric for management to consider when reviewing a project portfolio?

A. Cost of projects divided by total IT cost
B. Expected return divided by total project cost
C. Net present value (NPV) of the portfolio
D. Total cost of each project

Correct Answer: C
Section:
Explanation:
The most useful metric for management to consider when reviewing a project portfolio is the net present value (NPV) of the portfolio. NPV is a measure of the profitability and value of a project or a portfolio of projects,

taking into account the time value of money and the expected cash flows.NPV compares the present value of the future cash inflows with the present value of the initial investment and shows how much value is created or lost by undertaking a project or a portfolio of projects1. A positive NPV indicates that the project or portfolio is worth more than its cost and will generate a positive return on investment. A negative NPV indicates that the project or portfolio is worth less than its cost and will result in a loss.Therefore, NPV helps management to prioritize and select the most profitable and valuable projects or portfolios that align with the organizational strategy and objectives2. The other options are less useful or incorrect because:
A . Cost of projects divided by total IT cost is not a useful metric for reviewing a project portfolio, as it does not reflect the benefits, value, or return of the projects.It only shows the proportion of IT budget allocated to the projects, which may not be indicative of their strategic importance or alignment3.
B . Expected return divided by total project cost is not a useful metric for reviewing a project portfolio, as it does not account for the time value of money and the timing of cash flows.It only shows the average return per unit of cost, which may not be comparable across different projects or portfolios with different durations, risks, and cash flow patterns4.
D . Total cost of each project is not a useful metric for reviewing a project portfolio, as it does not reflect the benefits, value, or return of the projects.It only shows the initial investment required for each project, which may not be indicative of their profitability or viability5.Reference:Portfolio, Program and Project Management Using COBIT 5 - ISACA,Project Portfolio Management - ISACA,CISA Review Manual (Digital Version),Standards, Guidelines, Tools and Techniques

QUESTION 56
An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

A. Improve the change management process
B. Establish security metrics.
C. Perform a penetration test
D. Perform a configuration review

Correct Answer: D
Section:
Explanation:
The best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities is to perform a configuration review. A configuration review is an audit procedure that involves examining and verifying the security settings and parameters of application servers against predefined standards or best practices.A configuration review can help to identify and remediate any deviations, inconsistencies, or misconfigurations that may expose the application servers to unauthorized access, exploitation, or compromise6. A configuration review can also help to ensure compliance with security policies and regulations, as well as enhance the performance and availability of application servers. The other options are less effective or incorrect because:
A . Improving the change management process is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While improving the change management process may help to prevent future inconsistencies or misconfigurations in application server settings, it does not ensure that the existing ones are detected and corrected.
B . Establishing security metrics is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While establishing security metrics may help to measure and monitor the security performance and posture of application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected.
C . Performing a penetration test is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While performing a penetration test may help to simulate and evaluate the impact of an attack on application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected.Reference:Configuring system to use application server security - IBM,Application Security Risk: Assessment and Modeling - ISACA,Five Key Components of an Application Security Program - ISACA,ISACA Practitioner Guidelines for Auditors - SSH,SCADA Cybersecurity Framework - ISACA

QUESTION 57
Which of the following should an IS auditor expect to see in a network vulnerability assessment?

A. Misconfiguration and missing updates
B. Malicious software and spyware
C. Zero-day vulnerabilities
D. Security design flaws

Correct Answer: A
Section:
Explanation:

A network vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the network or its resources. A network vulnerability assessment typically involves scanning the network devices, such as routers, switches, firewalls, servers, and workstations, using automated tools that compare the device configurations, software versions, and patch levels against a database of known vulnerabilities. A network vulnerability assessment can also include manual testing and verification of the network architecture, design, policies, and procedures.One of the main objectives of a network vulnerability assessment is to detect and report any misconfiguration and missing updates in the network devices that could pose a security risk1. Misconfiguration refers to any deviation from the recommended or best practice settings for the network devices, such as weak passwords, open ports, unnecessary services, default accounts, or incorrect permissions.Missing updates refer to any outdated or unsupported software or firmware that has not been patched with the latest security fixes or enhancements from the vendors2.Misconfiguration and missing updates are common sources of network vulnerabilities that can be exploited by attackers to gain unauthorized access, execute malicious code, cause denial of service, or escalate privileges on the network devices3. Therefore, an IS auditor should expect to see misconfiguration and missing updates in a network vulnerability assessment. The other options are less relevant or incorrect because:
B . Malicious software and spyware are not usually detected by a network vulnerability assessment, as they are more related to the content and behavior of the network traffic rather than the configuration and patch level of the network devices. Malicious software and spyware are programs that infect or monitor the network devices or their users for malicious purposes, such as stealing data, displaying ads, or performing remote commands.Malicious software and spyware can be detected by other security tools, such as antivirus software, firewalls, or intrusion detection systems4.
C . Zero-day vulnerabilities are not usually detected by a network vulnerability assessment, as they are unknown or undisclosed vulnerabilities that have not been reported or patched by the vendors or the security community. Zero-day vulnerabilities are rare and difficult to discover, as they require advanced techniques and skills to exploit them.Zero-day vulnerabilities can be detected by other security tools, such as intrusion prevention systems, anomaly detection systems, or artificial intelligence systems5.

Security design flaws are not usually detected by a network vulnerability assessment, as they are more related to the logic and functionality of the network rather than the configuration and patch level of the network devices. Security design flaws are errors or weaknesses in the network architecture, design, policies, or procedures that could compromise the security objectives of the network.Security design flaws can be detected by other security methods, such as security reviews, audits, or assessments6.Reference:Network Vulnerability Assessment - ISACA,Network Vulnerability Scanning - NIST,Network Vulnerabilities - SANS,Malware - ISACA,Zero-Day Attacks - ISACA,Security Design Principles - NIST

QUESTION 58
An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

A. security parameters are set in accordance with the manufacturer s standards.
B. a detailed business case was formally approved prior to the purchase.
C. security parameters are set in accordance with the organization's policies.
D. the procurement project invited lenders from at least three different suppliers.

Correct Answer: C
Section:
Explanation:
The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies.Security parameters are settings or options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization's policies are documents that define the security goals, requirements, standards, and guidelines for the organization's information systems. An IS auditor should verify that security parameters are set in accordance with the organization's policies to ensure that the new server complies with the organization's security expectations and regulations. The other options are less important or incorrect because:
A . Security parameters should not be set in accordance with the manufacturer's standards alone, as they may not reflect the organization's specific security needs and environment. The manufacturer's standards are general recommendations or best practices for configuring the server's security parameters based on common scenarios and threats. An IS auditor should compare the manufacturer's standards with the organization's policies and identify any gaps or conflicts that need to be resolved.
B . A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.
D . The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization.Reference:Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA], [Business Case - ISACA], [Tender - ISACA], [Procurement Management - ISACA]

QUESTION 59
What is the PRIMARY benefit of an audit approach which requires reported findings to be issued together with related action plans, owners, and target dates?

A. it facilitates easier audit follow-up
B. it enforces action plan consensus between auditors and auditees

C. it establishes accountability for the action plans
D. it helps to ensure factual accuracy of findings

Correct Answer: C
Section:
Explanation:
The primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates is that it establishes accountability for the action plans. Accountability means that the individuals or groups who are responsible for implementing the action plans are clearly identified and held liable for their completion within the specified time frame.Accountability also implies that the action plans are monitored and evaluated to ensure that they are effective and efficient in addressing the audit findings and mitigating the associated risks1.Accountability helps to ensure that the audit recommendations are taken seriously and implemented properly, and that the audit value is realized by the organization2. The other options are less relevant or incorrect because:
A . It facilitates easier audit follow-up is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a secondary or indirect benefit.Audit follow-up is the process of verifying whether the action plans have been implemented and whether they have resolved the audit findings3. While having clear action plans, owners, and target dates may facilitate easier audit follow-up by providing a basis for tracking and reporting the progress and status of the action plans, it does not necessarily guarantee that the action plans will be implemented or effective.
B . It enforces action plan consensus between auditors and auditees is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a prerequisite or condition for such an approach.Action plan consensus means that the auditors and auditees agree on the audit findings and recommendations, and on the action plans to address them4. While having action plan consensus may enhance the credibility and acceptance of the audit approach, it does not necessarily ensure that the action plans will be implemented or effective.
D . It helps to ensure factual accuracy of findings is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of an outcome or result of such an approach.Factual accuracy of findings means that the audit findings are based on sufficient, reliable, relevant, and useful evidence5. While having factual accuracy of findings may increase the confidence and trust in the audit approach, it does not necessarily ensure that the action plans will be implemented or effective.Reference:Accountability - ISACA,Audit Value - ISACA,Audit Follow-up - ISACA,Action Plan Consensus - ISACA,Factual Accuracy of Findings - ISACA

QUESTION 60
During the planning phase of a data loss prevention (DLP) audit, management expresses a concern about mobile computing. Which of the following should the IS auditor identity as the associated risk?

A. The use of the cloud negatively impacting IT availably
B. Increased need for user awareness training
C. Increased vulnerability due to anytime, anywhere accessibility
D. Lack of governance and oversight for IT infrastructure and applications

Correct Answer: C
Section:
Explanation:
The associated risk of mobile computing that an IS auditor should identify during the planning phase of a data loss prevention (DLP) audit is increased vulnerability due to anytime, anywhere accessibility.Mobile computing refers to the use of portable devices, such as laptops, tablets, smartphones, or wearable devices, that can access data and applications over wireless networks from any location6. Mobile computing enables greater flexibility, productivity, and convenience for users, but also poses significant security challenges for organizations. One of these challenges is increased vulnerability due to anytime, anywhere accessibility.This means that mobile devices are exposed to a higher risk of loss, theft, damage, or unauthorized access than stationary devices7.If mobile devices contain or access sensitive data without proper protection, such as encryption or authentication, they could result in data leakage or breach in case of compromise8. Therefore, an IS auditor should identify this risk as part of a DLP audit. The other options are less relevant or incorrect because:
A . The use of cloud negatively impacting IT availability is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more related to cloud computing than mobile computing. Cloud computing refers to the delivery of computing services, such as data storage or processing, over the Internet from remote servers. Cloud computing may enable or support mobile computing by providing access to data and applications from any device or location, but it does not necessarily imply mobile computing. The use of cloud may negatively impact IT availability if there are disruptions or outages in the cloud service provider's network or infrastructure, but this is not a direct consequence of mobile computing.
B . Increased need for user awareness training is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a control or mitigation measure than a risk. User awareness training refers to educating users about security policies, procedures, and best practices for using mobile devices and protecting data. User awareness training may help to reduce the risk of data loss or breach due to mobile computing by increasing user knowledge and responsibility, but it does not eliminate or prevent the risk.
D . Lack of governance and oversight for IT infrastructure and applications is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a general or organizational risk than a specific or technical risk. Governance and oversight refer to the establishment and implementation of policies, standards, and procedures for managing IT resources and aligning them with business objectives. Lack of governance and oversight for IT infrastructure and applications may affect the security and performance of mobile devices and data, but it is not a direct or inherent result of mobile computing.Reference:Mobile Computing - ISACA,Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous - ISACA,Data Loss Prevention---Next Steps - ISACA, [Cloud Computing - ISACA], [Cloud Computing Risk Assessment - ISACA], [User Awareness Training - ISACA], [Governance and Oversight - ISACA]

QUESTION 61
Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

A. Analyzing risks posed by new regulations
B. Developing procedures to monitor the use of personal data
C. Defining roles within the organization related to privacy
D. Designing controls to protect personal data

Correct Answer: A
Section:
Explanation:
An appropriate role of internal audit in helping to establish an organization's privacy program is analyzing risks posed by new regulations. A privacy program is a set of policies, procedures, and controls that aim to protect the personal data of individuals from unauthorized or unlawful collection, use, disclosure, or disposal. A privacy program should comply with the applicable laws and regulations that govern the privacy rights and obligations of individuals and organizations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). New regulations may introduce new requirements or changes that affect the organization's privacy program and expose it to potential compliance risks or penalties.Therefore, internal audit can help to establish an organization's privacy program by analyzing the risks posed by new regulations and providing assurance, advice, or recommendations on how to address them1. The other options are less appropriate or incorrect because:
B . Developing procedures to monitor the use of personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity.Internal audit should provide assurance on the effectiveness and efficiency of the organization's privacy program, but not create or execute it2.
C . Defining roles within the organization related to privacy is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a governance or strategic role. Internal audit should not be involved in setting or approving the organization's privacy strategy, objectives, or policies, as it would compromise its independence and objectivity.Internal audit should provide assurance on the alignment and compliance of the organization's privacy program with its strategy, objectives, and policies, but not define or approve them2.
D . Designing controls to protect personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity.Internal audit should provide assurance on the adequacy and effectiveness of the organization's privacy program, but not design or implement it2.Reference:ISACA Introduces New Audit Programs for Business Continuity/Disaster ...,Best Practices for Privacy Audits - ISACA,ISACA Produces New Audit and Assurance Programs for Data Privacy and ...

QUESTION 62
Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

A. The BCP's contact information needs to be updated
B. The BCP is not version controlled.
C. The BCP has not been approved by senior management.
D. The BCP has not been tested since it was first issued.

Correct Answer: D
Section:
Explanation:
The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster.A BCP should include information such as roles and responsibilities, recovery strategies, resources, procedures, communication plans, and backup arrangements3. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements.Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident4. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:
A . The BCP's contact information needs to be updated is not a great concern for an IS auditor reviewing an organization's BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.
B . The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization's BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or

effectiveness of the BCP.
C . The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization's BCP, as it is a high-level issue that can be resolved. Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization. Approval by senior management helps to ensure that the BCP is aligned with the organization's strategy, objectives, and priorities, and that it has sufficient resources and authority to be implemented. Approval by senior management also helps to increase the awareness and commitment of the organization's stakeholders to the BCP. While having no approval by senior management may affect the credibility and acceptance of the BCP, it does not affect the overall validity or effectiveness of the BCP.Reference:Working Toward a Managed, Mature Business Continuity Plan - ISACA,ISACA Introduces New Audit Programs for Business Continuity/Disaster ...,Disaster Recovery and Business Continuity Preparedness for Cloud-based ...

QUESTION 63
A post-implementation review was conducted by issuing a survey to users. Which of the following should be of GREATEST concern to an IS auditor?

A. The survey results were not presented in detail lo management.
B. The survey questions did not address the scope of the business case.
C. The survey form template did not allow additional feedback to be provided.
D. The survey was issued to employees a month after implementation.

Correct Answer: B
Section:
Explanation:
The greatest concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users is that the survey questions did not address the scope of the business case. A post-implementation review is a process of evaluating the outcomes and benefits of a project after it has been completed and implemented.A post-implementation review can help to assess whether the project met its objectives, delivered its expected value, and satisfied its stakeholders1. A survey is a method of collecting feedback and opinions from users or other stakeholders about their experience and satisfaction with the project.A survey can help to measure the user acceptance, usability, and functionality of the project deliverables2. A business case is a document that justifies the need for a project based on its expected benefits, costs, risks, and alternatives.A business case defines the scope, objectives, and requirements of the project and provides a basis for its approval and initiation3. Therefore, an IS auditor should be concerned if the survey questions did not address the scope of the business case, as it may indicate that the post-implementation review was not comprehensive, relevant, or aligned with the project goals. The other options are less concerning or incorrect because:
A . The survey results were not presented in detail to management is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a communication or reporting issue than an audit issue. While presenting the survey results in detail to management may help to inform them about the project performance and outcomes, it does not affect the validity or quality of the post-implementation review itself.
C . The survey form template did not allow additional feedback to be provided is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a design or format issue than an audit issue. While allowing additional feedback to be provided may help to capture more insights or suggestions from users, it does not affect the validity or quality of the post-implementation review itself.
D . The survey was issued to employees a month after implementation is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a timing or scheduling issue than an audit issue. While issuing the survey to employees sooner after implementation may help to collect more accurate and timely feedback from users, it does not affect the validity or quality of the post-implementation review itself.Reference:Post Implementation Review - ISACA,Survey - ISACA,Business Case - ISACA

QUESTION 64
Which of the following is the BEST reason to implement a data retention policy?

A. To limit the liability associated with storing and protecting information
B. To document business objectives for processing data within the organization
C. To assign responsibility and ownership for data protection outside IT
D. To establish a recovery point detective (RPO) for (toaster recovery procedures

Correct Answer: A
Section:
Explanation:
The best reason to implement a data retention policy is to limit the liability associated with storing and protecting information. A data retention policy is a document that defines how long data should be kept by an organization and how they should be disposed of when they are no longer needed.A data retention policy should comply with the applicable laws and regulations that govern the data retention requirements and obligations of organizations, such as tax laws, privacy laws, or industry standards4.Implementing a data retention policy can help to limit the liability associated with storing and protecting information by reducing the amount of data that need to be stored and secured, minimizing the risk of data breaches or leaks, ensuring compliance with legal or contractual obligations, and avoiding potential fines or penalties for non-compliance5. The other options are

less relevant or incorrect because:
B . Documenting business objectives for processing data within the organization is not a reason to implement a data retention policy, as it is more related to data governance than data retention. Data governance refers to the policies, procedures, and controls that define how data are collected, used, managed, and shared within an organization.Data governance helps to ensure that data are aligned with business objectives and support decision making6.
C . Assigning responsibility and ownership for data protection outside IT is not a reason to implement a data retention policy, as it is more related to data accountability than data retention. Data accountability refers to the identification and assignment of roles and responsibilities for data protection among different stakeholders within an organization.Data accountability helps to ensure that data are handled appropriately and securely by authorized parties7.
D . Establishing a recovery point objective (RPO) for disaster recovery procedures is not a reason to implement a data retention policy, as it is more related to data backup than data retention. Data backup refers to the process of creating copies of data that can be restored in case of data loss or corruption.Data backup helps to ensure that data are available and recoverable in case of disaster8.RPO is a measure of the maximum amount of data that can be lost or acceptable in case of disaster9.Reference:Data Retention Policy - ISACA,Data Retention - ISACA,Data Governance - ISACA,Data Accountability - ISACA,Data Backup - ISACA,Recovery Point Objective - ISACA

QUESTION 65
Which of the following would MOST effectively help to reduce the number of repealed incidents in an organization?

A. Testing incident response plans with a wide range of scenarios
B. Prioritizing incidents after impact assessment.
C. Linking incidents to problem management activities
D. Training incident management teams on current incident trends

Correct Answer: C
Section:
Explanation:
Linking incidents to problem management activities would most effectively help to reduce the number of repeated incidents in an organization, because problem management aims to identify and eliminate the root causes of incidents and prevent their recurrence. Testing incident response plans, prioritizing incidents, and training incident management teams are all good practices, but they do not directly address the issue of repeated incidents.Reference:ISACA ITAF 3rd Edition Section 3600

QUESTION 66
Which of the following is the MOST significant risk that IS auditors are required to consider for each engagement?

A. Process and resource inefficiencies
B. Irregularities and illegal acts
C. Noncompliance with organizational policies
D. Misalignment with business objectives

Correct Answer: D
Section:
Explanation:
The most significant risk that IS auditors are required to consider for each engagement is the misalignment with business objectives. This is because IS audit engagements are intended to provide assurance that the IT systems and processes support the achievement of the business objectives and strategies.If there is a misalignment, it could result in wasted resources, missed opportunities, inefficiencies, errors, or failures that could adversely affect the organization's performance and reputation12.Reference:1: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.3: Audit Risk, page 282: CISA Online Review Course, Module 1: The Process of Auditing Information Systems, Lesson 1.3: Audit Risk

QUESTION 67
An externally facing system containing sensitive data is configured such that users have either read-only or administrator rights. Most users of the system have administrator access. Which of the following is the GREATEST risk associated with this situation?

A. Users can export application logs.
B. Users can view sensitive data.

C. Users can make unauthorized changes.
D. Users can install open-licensed software.

Correct Answer: C
Section:
Explanation:
The greatest risk associated with having most users with administrator access to an externally facing system containing sensitive data is that users can make unauthorized changes to the system or the data, which could compromise the integrity, confidentiality, and availability of the system and the data. Users can export application logs, view sensitive data, and install open-licensed software are also risks, but they are not as severe as unauthorized changes.Reference:ISACA CISA Review Manual 27th Edition Chapter 4

QUESTION 68
During an audit of an organization's risk management practices, an IS auditor finds several documented IT risk acceptances have not been renewed in a timely manner after the assigned expiration date When assessing the seventy of this finding, which mitigating factor would MOST significantly minimize the associated impact?

A. There are documented compensating controls over the business processes.
B. The risk acceptances were previously reviewed and approved by appropriate senior management
C. The business environment has not significantly changed since the risk acceptances were approved.
D. The risk acceptances with issues reflect a small percentage of the total population

Correct Answer: A
Section:
Explanation:
The mitigating factor that would most significantly minimize the impact of not renewing IT risk acceptances in a timely manner is having documented compensating controls over the business processes. Compensating controls are alternative controls that reduce or eliminate the risk when the primary control is not feasible or cost-effective. The other factors, such as previous approval by senior management, unchanged business environment, and small percentage of issues, do not mitigate the risk as effectively as compensating controls.Reference:ISACA CISA Review Manual 27th Edition Chapter 1

QUESTION 69
Which of the following is the MOST effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented?

A. Ensure sufficient audit resources are allocated,
B. Communicate audit results organization-wide.
C. Ensure ownership is assigned.
D. Test corrective actions upon completion.

Correct Answer: C
Section:
Explanation:
The most effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented is to ensure ownership is assigned. This means that the management of the audited area should accept responsibility for implementing the action plans and report on their progress and completion to the audit committee or senior management.This will ensure accountability, commitment, and follow-up for the audit recommendations34.Reference:3: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.6: Reporting, page 414: CISA Online Review Course, Module 1: The Process of Auditing Information Systems, Lesson 1.6: Reporting

QUESTION 70
Which of the following is the BEST metric to measure the alignment of IT and business strategy?

A. Level of stakeholder satisfaction with the scope of planned IT projects
B. Percentage of enterprise risk assessments that include IT-related risk
C. Percentage of stat satisfied with their IT-related roles

D. Frequency of business process capability maturity assessments

Correct Answer: B
Section:
Explanation:
The best metric to measure the alignment of IT and business strategy is the percentage of enterprise risk assessments that include IT-related risk. This metric indicates how well the organization identifies and manages the IT risks that could affect its strategic objectives and performance. A high percentage of enterprise risk assessments that include IT-related risk shows that the organization considers IT as an integral part of its business strategy and aligns its IT resources and capabilities with its business needs and goals .Reference:: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.2: IT Strategy, page 67 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.2: IT Strategy

QUESTION 71
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA> to automate routine business tasks?

A. The end-to-end process is understood and documented.
B. Roles and responsibilities are defined for the business processes in scope.
C. A benchmarking exercise of industry peers who use RPA has been completed.
D. A request for proposal (RFP) has been issued to qualified vendors.

Correct Answer: A
Section:
Explanation:
The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows.Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures12.Without a proper documentation of the end-to-end process, the organization may face challenges in designing, developing, testing, deploying, and monitoring the RPA solution3.Reference:1: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 2112: CISA Online Review Course, Module 4: Information Systems Operations and Business Resilience, Lesson 4.2: IT Service Delivery and Support3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

QUESTION 72
Which of the following should be performed FIRST before key performance indicators (KPIs) can be implemented?

A. Analysis of industry benchmarks
B. Identification of organizational goals
C. Analysis of quantitative benefits
D. Implementation of a balanced scorecard

Correct Answer: B
Section:
Explanation:
The first thing that should be performed before key performance indicators (KPIs) can be implemented is the identification of organizational goals.This is because KPIs are measurable values that demonstrate how effectively an organization is achieving its key business objectives4. Therefore, it is necessary that the organization defines its goals clearly and aligns them with its vision, mission, and strategy.By identifying its goals, the organization can then determine what KPIs are relevant and meaningful to measure its progress and performance .Reference:4: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.3: Benefits Realization, page 77 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.3: Benefits Realization : ISACA Journal Volume 1, 2020, Article: How to Measure Anything in IT Governance

QUESTION 73
During audit framework. an IS auditor teams that employees are allowed to connect their personal devices to company-owned computers. How can the auditor BEST validate that appropriate security controls are in place to prevent data loss?

A. Conduct a walk-through to view results of an employee plugging in a device to transfer confidential data.
B. Review compliance with data loss and applicable mobile device user acceptance policies.
C. Verify the data loss prevention (DLP) tool is properly configured by the organization.
D. Verify employees have received appropriate mobile device security awareness training.

Correct Answer: B
Section:
Explanation:
The best way to validate that appropriate security controls are in place to prevent data loss is to review compliance with data loss and applicable mobile device user acceptance policies. This will ensure that the organization has established clear rules and guidelines for employees to follow when connecting their personal devices to company-owned computers. A walk-through, a DLP tool configuration, and a security awareness training are not sufficient to validate the effectiveness of the controls, as they may not cover all possible scenarios and risks.Reference:IT Audit Fundamentals Certificate Resources

QUESTION 74
If enabled within firewall rules, which of the following services would present the GREATEST risk?

A. Simple mail transfer protocol (SMTP)
B. Simple object access protocol (SOAP)
C. Hypertext transfer protocol (HTTP)
D. File transfer protocol (FTP)

Correct Answer: D
Section:
Explanation:
File transfer protocol (FTP) is a service that allows users to transfer files between computers over a network. If enabled within firewall rules, FTP would present the greatest risk, as it can expose sensitive data to unauthorized access, modification, or deletion. FTP does not provide encryption or authentication, which makes it vulnerable to eavesdropping, spoofing, and tampering attacks. Simple mail transfer protocol (SMTP), simple object access protocol (SOAP), and hypertext transfer protocol (HTTP) are also services that can be used to exchange data over a network, but they have more security features than FTP, such as encryption, authentication, or validation.Reference:CISA Review Manual (Digital Version)

QUESTION 75
Which of the following is the BEST way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC)?

A. Have an independent party review the source calculations
B. Execute copies of EUC programs out of a secure library
C. implement complex password controls
D. Verify EUC results through manual calculations

Correct Answer: B
Section:
Explanation:
The best way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC) is to execute copies of EUC programs out of a secure library. This will ensure that the original EUC programs are protected from unauthorized changes and that the copies are run in a controlled environment. A secure library is a repository of EUC programs that have been tested, validated, and approved by the appropriate authority. Executing copies of EUC programs out of a secure library can also help with version control, backup, and recovery of EUC programs. Having an independent party review the source calculations, implementing complex password controls, and verifying EUC results through manual calculations are not as effective as executing copies of EUC programs out of a secure library, as they do not prevent or detect unintentional modifications of complex calculations in EUC.Reference:End-User Computing (EUC) Risks: A Comprehensive Guide,End User Computing (EUC) Risk Management

QUESTION 76
Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

A. Project segments are established.
B. The work is separated into phases.
C. The work is separated into sprints.
D. Project milestones are created.

Correct Answer: C
Section:
Explanation:
The best way to enable the effectiveness of an agile project for the rapid development of a new software application is to separate the work into sprints. Sprints are short, time-boxed iterations that deliver a potentially releasable product increment at the end of each sprint. Sprints allow agile teams to work in a flexible and adaptive manner, respond quickly to changing customer needs and feedback, and deliver value faster and more frequently. Sprints also help teams to plan, execute, review, and improve their work in a collaborative and transparent way. Project segments, phases, and milestones are not specific to agile projects and do not necessarily enable the effectiveness of an agile project.Reference:Agile Project Management [What is it & How to Start] - Atlassian,CISA Review Manual (Digital Version).

QUESTION 77
Which of the following would BEST ensure that a backup copy is available for restoration of mission critical data after a disaster''

A. Use an electronic vault for incremental backups
B. Deploy a fully automated backup maintenance system.
C. Periodically test backups stored in a remote location
D. Use both tape and disk backup systems

Correct Answer: C
Section:
Explanation:
The best way to ensure that a backup copy is available for restoration of mission critical data after a disaster is to periodically test backups stored in a remote location. Testing backups is essential to verify that the backup copies are valid, complete, and recoverable. Testing backups also helps to identify any issues or errors that may affect the backup process or the restoration of data. Storing backups in a remote location is important to protect the backup copies from physical damage, theft, or unauthorized access that may occur at the primary site. Using an electronic vault for incremental backups, deploying a fully automated backup maintenance system, or using both tape and disk backup systems are not sufficient to ensure that a backup copy is available for restoration of mission critical data after a disaster, as they do not address the need for testing backups or storing them in a remote location.Reference:Backup and Recovery of Data: The Essential Guide | Veritas,The Truth About Data Backup for Mission-Critical Environments - DATAVERSITY.

QUESTION 78
Which of the following is the BEST way to ensure that an application is performing according to its specifications?

A. Unit testing
B. Pilot testing
C. System testing
D. Integration testing

Correct Answer: D
Section:
Explanation:
Integration testing is the best way to ensure that an application is performing according to its specifications, because it tests the interaction and compatibility of different modules or components of the application.Unit testing, pilot testing and system testing are also important, but they do not cover the whole functionality and integration of the application as well as integration testing does.Reference:CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

QUESTION 79
Which of the following is the BEST evidence that an organization's IT strategy is aligned lo its business objectives?

A. The IT strategy is modified in response to organizational change.
B. The IT strategy is approved by executive management.
C. The IT strategy is based on IT operational best practices.
D. The IT strategy has significant impact on the business strategy

Correct Answer: B
Section:
Explanation:
The best evidence that an organization's IT strategy is aligned to its business objectives is that the IT strategy is approved by executive management. This implies that the IT strategy has been reviewed and validated by the senior leaders of the organization, who are responsible for setting and overseeing the business objectives.The IT strategy may be modified in response to organizational change, based on IT operational best practices, or have significant impact on the business strategy, but these are not sufficient indicators of alignment without executive approval.Reference:CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

QUESTION 80
Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

A. Perimeter firewall
B. Data loss prevention (DLP) system
C. Web application firewall
D. Network segmentation

Correct Answer: D
Section:
Explanation:
Network segmentation is the best security measure to reduce the risk of propagation when a cyberattack occurs, because it divides the network into smaller subnetworks that are isolated from each other and have different access controls and security policies. This limits the spread of malicious traffic and prevents attackers from accessing sensitive data or systems in other segments.A perimeter firewall, a data loss prevention (DLP) system, and a web application firewall are also useful security measures, but they do not prevent propagation within the network as effectively as network segmentation does.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

QUESTION 81
A credit card company has decided to outsource the printing of customer statements It Is MOST important for the company to verify whether:

A. the provider has alternate service locations.
B. the contract includes compensation for deficient service levels.
C. the provider's information security controls are aligned with the company's.
D. the provider adheres to the company's data retention policies.

Correct Answer: C
Section:
Explanation:
The most important thing for the company to verify when outsourcing the printing of customer statements is whether the provider's information security controls are aligned with the company's. This is because customer statements contain sensitive personal and financial information that need to be protected from unauthorized access, disclosure, modification or destruction. The provider's information security controls should be consistent with the company's policies, standards and regulations, and should be audited periodically to ensure compliance.The other options are also relevant, but not as critical as information security.Reference:CISA Review Manual (Digital Version)1, Chapter 3, Section 3.2.2

QUESTION 82
Which of the following would BEST help to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software?

A. Assign the security risk analysis to a specially trained member of the project management office.

B. Deploy changes in a controlled environment and observe for security defects.
C. Include a mandatory step to analyze the security impact when making changes.
D. Mandate that the change analyses are documented in a standard format.

Correct Answer: C
Section:
Explanation:
The best way to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software is to include a mandatory step to analyze the security impact when making changes. This will help to identify and mitigate any security risks or vulnerabilities that may arise from the changes, and to ensure that the software meets the security requirements and standards.The other options are not as effective, because they either delegate the security analysis to someone outside the development team, rely on post-deployment testing, or focus on documentation rather than analysis.Reference:CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.5

QUESTION 83
When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system. It is MOST effective for an IS auditor to review;

A. data analytics findings.
B. audit trails
C. acceptance lasting results
D. rollback plans

Correct Answer: A
Section:
Explanation:
When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system, it is most effective for an IS auditor to review data analytics findings. Data analytics is a technique that uses software tools and statistical methods to analyze large volumes of data and identify patterns, anomalies, errors or inconsistencies. Data analytics can help to compare the source and target data sets, validate the data quality and integrity, and detect any data loss or corruption during the migration process.The other options are not as effective, because audit trails only record the actions performed on the data, acceptance testing results only verify the functionality of the new system, and rollback plans only provide contingency measures in case of migration failure.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.6

QUESTION 84
An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

A. The quality of the data is not monitored.
B. Imported data is not disposed frequently.
C. The transfer protocol is not encrypted.
D. The transfer protocol does not require authentication.

Correct Answer: A
Section:
Explanation:
The most critical finding that the IS auditor should consider when reviewing processes for importing market price data from external data providers is that the quality of the data is not monitored. This is because market price data is essential for financial transactions, risk management, valuation and reporting, and any errors or inaccuracies in the data can have significant impact on the organization's performance, reputation and compliance. The IS auditor should ensure that the organization has established quality criteria and controls for the imported data, such as validity, completeness, timeliness, consistency and accuracy, and that the data is regularly checked and verified against these criteria.The other findings are also important, but not as critical as data quality.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

QUESTION 85
Which of the following would be of GREATEST concern when reviewing an organization's security information and event management (SIEM) solution?

A. SIEM reporting is customized.

B. SIEM configuration is reviewed annually
C. The SIEM is decentralized.
D. SIEM reporting is ad hoc.

Correct Answer: C
Section:
Explanation:
The greatest concern that the IS auditor should have when reviewing an organization's security information and event management (SIEM) solution is that the SIEM is decentralized. This is because a decentralized SIEM can pose challenges for collecting, correlating, analyzing and reporting on security events and incidents from multiple sources and locations. A decentralized SIEM can also increase the complexity and cost of maintaining and updating the SIEM components, as well as the risk of inconsistent or incomplete security monitoring and response. The IS auditor should recommend that the organization adopts a centralized or hybrid SIEM architecture that can provide a holistic and integrated view of the security posture and activities across the organization.The other findings are not as concerning as a decentralized SIEM, because they can be addressed by implementing best practices and standards for SIEM reporting and configuration.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

QUESTION 86
Which of the following is MOST important for an IS auditor to look for in a project feasibility study?

A. An assessment of whether requirements will be fully met
B. An assessment indicating security controls will operate effectively
C. An assessment of whether the expected benefits can be achieved
D. An assessment indicating the benefits will exceed the implement

Correct Answer: C
Section:
Explanation:
The most important thing for an IS auditor to look for in a project feasibility study is an assessment of whether the expected benefits can be achieved. A project feasibility study is a preliminary analysis that evaluates the viability and suitability of a proposed project based on various criteria, such as technical, economic, legal, operational, and social factors. The expected benefits are the positive outcomes and value that the project aims to deliver to the organization and its stakeholders. The IS auditor should verify whether the project feasibility study has clearly defined and quantified the expected benefits, and whether it has assessed the likelihood and feasibility of achieving them within the project scope, budget, schedule, and quality parameters.The other options are also important for an IS auditor to look for in a project feasibility study, but not as important as an assessment of whether the expected benefits can be achieved, because they either focus on specific aspects of the project rather than the overall value proposition, or they assume that the project will be implemented rather than evaluating its viability.Reference:CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.1

QUESTION 87
What should an IS auditor do FIRST when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective?

A. Determine the resources required to make the control effective.
B. Validate the overall effectiveness of the internal control.
C. Verify the impact of the control no longer being effective.
D. Ascertain the existence of other compensating controls.

Correct Answer: D
Section:
Explanation:
The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness.The other options are not the first steps, because they either require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls.Reference:CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

QUESTION 88

Which of the following should an IS auditor ensure is classified at the HIGHEST level of sensitivity?

A. Server room access history
B. Emergency change records
C. IT security incidents
D. Penetration test results

Correct Answer: D
Section:
Explanation:
The IS auditor should ensure that penetration test results are classified at the highest level of sensitivity, because they contain detailed information about the vulnerabilities and weaknesses of the IT systems and networks, as well as the methods and tools used by the testers to exploit them. Penetration test results can be used by malicious actors to launch cyberattacks or cause damage to the organization if they are disclosed or accessed without authorization. Therefore, they should be protected with the highest level of confidentiality, integrity and availability.The other options are not as sensitive as penetration test results, because they either do not reveal as much information about the IT security posture, or they are already known or reported by the organization.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

QUESTION 89
During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed. Which of the following is the BEST way to help management understand the associated risk?

A. Explain the impact to disaster recovery.
B. Explain the impact to resource requirements.
C. Explain the impact to incident management.
D. Explain the impact to backup scheduling.

Correct Answer: A
Section:
Explanation:
The best way to help management understand the associated risk of missing backup cycles due to operator error and lack of exception management is to explain the impact to disaster recovery. Disaster recovery is the process of restoring normal operations and functions after a disruptive event, such as a natural disaster, a cyberattack, or a hardware failure. Backup cycles are essential for disaster recovery, because they ensure that the organization has copies of its critical data and systems that can be restored in case of data loss or corruption. If backup cycles are missed due to operator error, and these exceptions are not managed, the organization may not have the latest or complete backups available for disaster recovery, which can result in prolonged downtime, reduced productivity, lost revenue, reputational damage, and legal or regulatory penalties.The other options are not as effective as explaining the impact to disaster recovery, because they either do not address the risk of data loss or corruption, or they focus on operational or technical aspects rather than business outcomes.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

QUESTION 90
Which of the following presents the GREATEST challenge to the alignment of business and IT?

A. Lack of chief information officer (CIO) involvement in board meetings
B. Insufficient IT budget to execute new business projects
C. Lack of information security involvement in business strategy development
D. An IT steering committee chaired by the chief information officer (CIO)

Correct Answer: A
Section:
Explanation:
The greatest challenge to the alignment of business and IT is the lack of chief information officer (CIO) involvement in board meetings. The CIO is the senior executive responsible for overseeing the IT strategy, governance, and operations of the organization, and ensuring that they support the business objectives and needs. The CIO should be involved in board meetings to communicate the value and contribution of IT to the organization, to align the IT vision and direction with the business strategy and priorities, and to advocate for the IT resources and investments required to achieve the desired outcomes. The lack of CIO involvement in board meetings can

result in a disconnect between business and IT, a loss of trust and confidence in IT, and missed opportunities for innovation and value creation.The other options are not as challenging as the lack of CIO involvement in board meetings, because they either do not affect the strategic alignment of business and IT, or they can be addressed by other means such as collaboration, negotiation, or escalation.Reference:CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

QUESTION 91
Which of the following is the MOST efficient way to identify segregation of duties violations in a new system?

A. Review a report of security rights in the system.
B. Observe the performance of business processes.
C. Develop a process to identify authorization conflicts.
D. Examine recent system access rights violations.

Correct Answer: A
Section:
Explanation:
The most efficient way to identify segregation of duties violations in a new system is to review a report of security rights in the system. Segregation of duties is a control principle that aims to prevent or detect errors, fraud, or abuse by ensuring that no single individual has the ability to perform incompatible or conflicting functions or activities within a system or process. A report of security rights in the system can provide a comprehensive and accurate overview of the roles, responsibilities, and access levels assigned to different users or groups in the system, and can help to identify any potential segregation of duties violations or risks.The other options are not as efficient as reviewing a report of security rights in the system, because they either rely on observation or testing rather than analysis, or they focus on existing rather than potential violations.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

QUESTION 92
An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?

A. Network penetration tests are not performed
B. The network firewall policy has not been approved by the information security officer.
C. Network firewall rules have not been documented.
D. The network device inventory is incomplete.

Correct Answer: A
Section:
Explanation:
The finding that should be ranked as the highest risk is that network penetration tests are not performed. Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices. Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If network penetration tests are not performed, the organization may not be aware of the existing or potential threats and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties.The other findings are also important, but not as risky as the lack of network penetration tests, because they either do not directly affect the network security controls, or they can be addressed by documentation or approval processes.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

QUESTION 93
An IS auditor is reviewing logical access controls for an organization's financial business application Which of the following findings should be of GREATEST concern to the auditor?

A. Users are not required to change their passwords on a regular basis
B. Management does not review application user activity logs
C. User accounts are shared between users
D. Password length is set to eight characters

Correct Answer: C

Section:
Explanation:
The finding that should be of greatest concern to the IS auditor is that user accounts are shared between users. User accounts are unique identifiers that grant access to an organization's financial business application based on the roles and responsibilities of the users. User accounts should be individualized and personalized to ensure accountability, traceability, and auditability of user actions and transactions. User accounts should not be shared between users, because this can compromise the confidentiality, integrity, and availability of the financial data and systems, and can enable unauthorized or fraudulent activities. If user accounts are shared between users, the IS auditor may not be able to determine who performed what action or transaction, or whether the user had the appropriate authorization or approval.The other findings are also concerning, but not as much as user account sharing, because they either affect the password strength or frequency rather than the user identity, or they relate to monitoring rather than controlling user access.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2
Topic 4, Exam Pool D (NEW)

QUESTION 94
Which of the following is MOST important for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan?

A. Strategic: goals have been considered.
B. A rollback plan is included.
C. A code check review is included.
D. A migration steering committee has been formed.

Correct Answer: B
Section:
Explanation:
The most important thing for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan is that a rollback plan is included. A rollback plan is a contingency plan that describes the steps and actions to be taken in case the data conversion or infrastructure migration fails or causes unacceptable problems or risks. A rollback plan can help to restore the original data and infrastructure, minimize the impact on the business operations and functions, and ensure the continuity and availability of the IT services. The IS auditor should verify that the rollback plan is feasible, tested, documented, and approved, and that it covers all the possible scenarios and outcomes of the data conversion or infrastructure migration.The other options are not as important as verifying the rollback plan, because they either do not address the potential failure or disruption of the data conversion or infrastructure migration, or they are part of the normal planning and execution process rather than a contingency plan.Reference:CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

QUESTION 95
Which of the following should be the FIRST step m managing the impact of a recently discovered zero-day attack?

A. Evaluating the likelihood of attack
B. Estimating potential damage
C. Identifying vulnerable assets
D. Assessing the Impact of vulnerabilities

Correct Answer: C
Section:
Explanation:
The first step in managing the impact of a recently discovered zero-day attack is to identify vulnerable assets. A zero-day attack is a cyberattack that exploits a previously unknown or unpatched vulnerability in a software or system, before the vendor or developer has had time to fix it. Identifying vulnerable assets is crucial for managing the impact of a zero-day attack, because it helps to determine the scope and severity of the attack, prioritize the protection and mitigation measures, and isolate or quarantine the affected assets from further damage or compromise.The other options are not the first steps in managing the impact of a zero-day attack, because they either require more information about the vulnerable assets, or they are part of the subsequent steps of assessing, responding, or recovering from the attack.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

QUESTION 96
Which of the following is me GREATE ST impact as a result of the ongoing deterioration of a detective control?

A. Increased number of false negatives in security logs
B. Decreased effectiveness of roof cause analysis
C. Decreased overall recovery time
D. Increased demand for storage space for logs

Correct Answer: A
Section:
Explanation:
The greatest impact as a result of the ongoing deterioration of a detective control is an increased number of false negatives in security logs. A detective control is a control that monitors and identifies any deviations or anomalies from the expected or normal behavior or performance of a system or process. A security log is a record of events or activities that occur within a system or network, such as user access, file changes, system errors, or security incidents. A false negative is a situation where a security log fails to detect or report an actual deviation or anomaly that has occurred, such as an unauthorized access, a malicious modification, or a security breach. An increased number of false negatives in security logs can have a significant impact on the organization's security posture and risk management, because it can prevent timely detection and response to security threats, compromise the accuracy and reliability of security monitoring and reporting, and undermine the accountability and auditability of user actions and transactions.The other options are not as impactful as an increased number of false negatives in security logs, because they either do not affect the detection capability of a detective control, or they have less severe consequences for security management.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

QUESTION 97
An auditee disagrees with a recommendation for corrective action that appears in the draft engagement report. Which of the following is the IS auditor's BEST course of action when preparing the final report?

A. Come to an agreement prior to issuing the final report.
B. Include the position supported by senior management in the final engagement report
C. Ensure the auditee's comments are included in the working papers
D. Exclude the disputed recommendation from the final engagement report

Correct Answer: B
Section:
Explanation:
The IS auditor's best course of action when preparing the final report is to include the position supported by senior management in the final engagement report. The IS auditor should communicate the audit findings and recommendations to senior management and obtain their feedback and approval before issuing the final report. If there is a disagreement between the auditee and the IS auditor regarding a recommendation for corrective action, the IS auditor should present both sides of the argument and the supporting evidence, and seek senior management's opinion and decision. The IS auditor should respect and follow senior management's position, and include it in the final engagement report, along with the auditee's comments if applicable.The other options are not the best course of action, because they either do not resolve the disagreement, do not reflect senior management's authority, or do not report the audit results accurately and completely.Reference:CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.5

QUESTION 98
Which of the following would provide the BEST evidence of an IT strategy corrections effectiveness?

A. The minutes from the IT strategy committee meetings
B. Synchronization of IT activities with corporate objectives
C. The IT strategy committee charier
D. Business unit satisfaction survey results

Correct Answer: B
Section:
Explanation:
The best evidence of an IT strategy correction's effectiveness is the synchronization of IT activities with corporate objectives. The IT strategy correction is a process of reviewing and adjusting the IT strategy to ensure that it aligns with and supports the corporate strategy and objectives. The synchronization of IT activities with corporate objectives means that the IT activities are consistent with and contribute to the achievement of the corporate goals and vision. The IS auditor can measure and evaluate the IT strategy correction's effectiveness by comparing the IT activities with the corporate objectives, and assessing whether they are aligned, integrated, and coordinated.The other options are not as good evidence of an IT strategy correction's effectiveness, because they either do not reflect the alignment of IT and business, or they are inputs or outputs of the IT strategy

correction process rather than outcomes or results.Reference:CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

QUESTION 99
An IT balanced scorecard is PRIMARILY used for:

A. evaluating the IT project portfolio
B. measuring IT strategic performance
C. allocating IT budget and resources
D. monitoring risk in lT-related processes

Correct Answer: B
Section:
Explanation:
An IT balanced scorecard is primarily used for measuring IT strategic performance. An IT balanced scorecard is a framework that translates the IT strategy into measurable objectives, indicators, targets, and initiatives across four perspectives: financial, customer, internal process, and learning and growth. An IT balanced scorecard helps to monitor and evaluate how well the IT function is delivering value to the organization, achieving its strategic goals, and improving its capabilities and competencies.The other options are not the primary uses of an IT balanced scorecard, because they either focus on specific aspects of IT rather than the overall performance, or they are not directly related to the IT strategy.Reference:CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.3

QUESTION 100
An IS auditor notes that not all security tests were completed for an online sales system recently promoted to production. Which of the following is the auditor's BEST course of action?

A. Determine exposure to the business
B. Adjust future testing activities accordingly
C. Increase monitoring for security incidents
D. Hire a third party to perform security testing

Correct Answer: A
Section:
Explanation:
The IS auditor's best course of action when reviewing the use of an outsourcer for disposal of storage media is to determine exposure to the business. Storage media, such as hard disks, tapes, flash drives, or CDs, may contain sensitive or confidential information that needs to be protected from unauthorized access, disclosure, or misuse. The IS auditor should verify that the outsourcer has a process that appropriately sanitizes the media before disposal, such as wiping, degaussing, shredding, or incinerating, and that the process is effective and compliant with the organization's policies and standards. The IS auditor should also assess the potential impact and risk to the business if the storage media is not properly sanitized or disposed of, such as data breaches, reputational damage, legal or regulatory penalties, or loss of competitive advantage.The other options are not the best course of action, because they either do not address the root cause of the problem, or they are reactive rather than proactive measures.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

QUESTION 101
Which of the following is MOST important for an IS auditor to verify when reviewing the use of an outsourcer for disposal of storage media?

A. The vendor's process appropriately sanitizes the media before disposal
B. The contract includes issuance of a certificate of destruction by the vendor
C. The vendor has not experienced security incidents in the past.
D. The disposal transportation vehicle is fully secure

Correct Answer: A
Section:
Explanation:
The most important thing for an IS auditor to verify when reviewing the use of an outsourcer for disposal of storage media is that the vendor's process appropriately sanitizes the media before disposal. As explained in the previous question, storage media may contain sensitive or confidential information that needs to be protected from unauthorized access, disclosure, or misuse. The IS auditor should verify that the vendor has a process that

appropriately sanitizes the media before disposal, such as wiping, degaussing, shredding, or incinerating, and that the process is effective and compliant with the organization's policies and standards.The other options are not as important as verifying the vendor's process, because they either do not ensure the security and privacy of the information on the media, or they are secondary to the vendor's process.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

QUESTION 102
An IS department is evaluated monthly on its cost-revenue ratio user satisfaction rate, and computer downtime This is BEST zed as an application of.

A. risk framework
B. balanced scorecard
C. value chain analysis
D. control self-assessment (CSA)

Correct Answer: B
Section:
Explanation:
. A balanced scorecard is a framework that translates the IT strategy into measurable objectives, indicators, targets, and initiatives across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard helps to monitor and evaluate how well the IT function is delivering value to the organization, achieving its strategic goals, and improving its capabilities and competencies. The other options are not the primary uses of a balanced scorecard, because they either focus on specific aspects of IT rather than the overall performance, or they are not directly related to the IT strategy.

QUESTION 103
Which of the following is the PRIMARY reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report?

A. To ensure the conclusions are adequately supported
B. To ensure adequate sampling methods were used during fieldwork
C. To ensure the work is properly documented and filed
D. To ensure the work is conducted according to industry standards

Correct Answer: A
Section:
Explanation:
The primary reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report is to ensure the conclusions are adequately supported. The IS audit manager is responsible for overseeing and supervising the audit process, ensuring the quality and consistency of the audit work, and approving the audit report and recommendations. The IS audit manager should review the work performed by the senior IS auditor to verify that the audit objectives, scope, and criteria have been met, that the audit evidence is sufficient, reliable, and relevant, and that the audit conclusions are logical, objective, and based on the audit evidence. The IS audit manager should also ensure that the audit report is clear, concise, accurate, and complete, and that it communicates the audit findings, conclusions, and recommendations effectively to the intended audience.The other options are not the primary reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report, because they either relate to specific aspects or stages of the audit work rather than the overall outcome, or they are part of the senior IS auditor's responsibility rather than the IS audit manager's.Reference:CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.5

QUESTION 104
Which of following is MOST important to determine when conducting a post-implementation review?

A. Whether the solution architecture compiles with IT standards
B. Whether success criteria have been achieved
C. Whether the project has been delivered within the approved budget
D. Whether lessons teamed have been documented

Correct Answer: B
Section:
Explanation:

The most important thing to determine when conducting a post-implementation review is whether success criteria have been achieved. A post-implementation review is a process of evaluating the results and outcomes of a project or initiative after it has been completed and implemented. The success criteria are the measurable indicators that define what constitutes a successful project or initiative in terms of its objectives, benefits, quality, performance, and stakeholder satisfaction. The IS auditor should verify whether the success criteria have been achieved by comparing the actual results and outcomes with the expected or planned ones, and by assessing whether they meet or exceed the expectations and requirements of the stakeholders. The IS auditor should also identify any gaps, issues, or risks that may affect the sustainability or scalability of the project or initiative, and provide recommendations for improvement or remediation.The other options are not as important as determining whether success criteria have been achieved when conducting a post-implementation review, because they either focus on specific aspects or components of the project or initiative rather than the overall value proposition, or they are part of the pre-implementation or implementation phases rather than the post-implementation phase.Reference:CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

QUESTION 105
Which of the following is the GREATEST risk if two users have concurrent access to the same database record?

A. Availability integrity
B. Data integrity
C. Entity integrity
D. Referential integrity

Correct Answer: B
Section:
Explanation:
The greatest risk if two users have concurrent access to the same database record is data integrity. Data integrity is the property that ensures that the data is accurate, complete, consistent, and valid throughout its lifecycle. If two users have concurrent access to the same database record, they may modify or delete the data in a conflicting or inconsistent manner, resulting in data corruption, loss, or duplication. This can affect the reliability and quality of the data, and cause errors or anomalies in the database operations and functions.The IS auditor should verify that the database has adequate controls to prevent or resolve concurrent access issues, such as locking mechanisms, transaction isolation levels, concurrency control protocols, or timestamping methods.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

QUESTION 106
The PRIMARY purpose of requiring source code escrow in a contractual agreement is to:

A. comply with vendor management policy
B. convert source code to new executable code.
C. satisfy regulatory requirements.
D. ensure the source code is available.

Correct Answer: D
Section:
Explanation:
The primary purpose of requiring source code escrow in a contractual agreement is to ensure the source code is available. Source code escrow is a service that involves depositing the source code of a software or system with a third-party agent or escrow provider, who can release it to a designated beneficiary under specific conditions, such as bankruptcy, termination, or breach of contract by the software vendor or developer. Source code escrow can help to protect the interests and rights of the software user or licensee, who may need access to the source code for maintenance, modification, enhancement, or troubleshooting purposes.The IS auditor should verify that the contractual agreement specifies the terms and conditions for source code escrow, such as the escrow agent, the escrow fees, the deposit frequency and format, the release events and procedures, and the verification and audit requirements.Reference:CISA Review Manual (Digital Version)1, Chapter 3, Section 3.2.2

QUESTION 107
Which of the following provides the MOST assurance of the integrity of a firewall log?

A. The log is reviewed on a monthly basis.
B. Authorized access is required to view the log.
C. The log cannot be modified.
D. The log is retained per policy.

Correct Answer: C
Section:
Explanation:
The best way to provide assurance of the integrity of a firewall log is to ensure that the log cannot be modified. A firewall log is a record of the traffic and events that occur at the firewall, which is a device or software that controls and filters the incoming and outgoing network traffic based on predefined rules and policies. The integrity of a firewall log means that the log is accurate, complete, consistent, and valid, and that it has not been altered, deleted, or corrupted by unauthorized or malicious parties. The IS auditor should verify that the firewall log has adequate controls to prevent or detect any modification of the log, such as encryption, hashing, digital signatures, write-once media, or tamper-evident seals.The other options are not as effective as ensuring that the log cannot be modified, because they either do not address the integrity of the log data, or they are monitoring or retention measures rather than preventive or detective controls.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

QUESTION 108
Which of the following is the BEST recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage?

A. Require employees to waive privacy rights related to data on BYOD devices.
B. Require multi-factor authentication on BYOD devices,
C. Specify employee responsibilities for reporting lost or stolen BYOD devices.
D. Allow only registered BYOD devices to access the network.

Correct Answer: B
Section:
Explanation:
The best recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage is to require multi-factor authentication on BYOD devices. BYOD is a practice that allows employees to use their own personal devices, such as smartphones, tablets, or laptops, to access the organization's network, data, and systems. Data leakage is a risk that involves the unauthorized or accidental disclosure or transfer of sensitive or confidential data from the organization to external parties or devices. Multi-factor authentication is a security measure that requires users to provide two or more pieces of evidence to verify their identity and access rights, such as passwords, tokens, biometrics, or codes. Multi-factor authentication can help prevent data leakage by reducing the likelihood of unauthorized access to the organization's data and systems through BYOD devices, especially if they are lost, stolen, or compromised.The other options are not as effective as requiring multi-factor authentication on BYOD devices, because they either do not prevent data leakage directly, or they are reactive rather than proactive measures.Reference:CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

QUESTION 109
Which of the following is the MOST appropriate control to ensure integrity of online orders?

A. Data Encryption Standard (DES)
B. Digital signature
C. Public key encryption
D. Multi-factor authentication

Correct Answer: B
Section:
Explanation:
A digital signature is the most appropriate control to ensure integrity of online orders because it provides a way to verify the authenticity and integrity of the data sent by the sender. A digital signature is created by applying a cryptographic algorithm to the data and attaching the result to the data. The receiver can then use the sender's public key to verify that the data has not been altered or tampered with during transmission. A digital signature also provides non-repudiation, which means that the sender cannot deny sending the data.
Data Encryption Standard (DES) is a symmetric encryption algorithm that can provide confidentiality of online orders, but not integrity. DES uses the same key to encrypt and decrypt the data, which means that anyone who has the key can modify the data without detection.
Public key encryption is an asymmetric encryption algorithm that can also provide confidentiality of online orders, but not integrity. Public key encryption uses a pair of keys: a public key and a private key. The sender encrypts the data with the receiver's public key, and the receiver decrypts it with their own private key. However, public key encryption does not prevent anyone from modifying the encrypted data.
Multi-factor authentication is a control that can provide authentication and authorization of online orders, but not integrity. Multi-factor authentication requires the user to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Multi-factor authentication can prevent unauthorized access to online orders, but it does not protect the data from being modified after being sent.
ISACA, CISA Review Manual, 27th Edition, 2019, p.2811
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

QUESTION 110
Which of the following provides the BEST evidence that a third-party service provider's information security controls are effective?

A. An audit report of the controls by the service provider's external auditor
B. Documentation of the service provider's security configuration controls
C. An interview with the service provider's information security officer
D. A review of the service provider's policies and procedures

Correct Answer: A
Section:
Explanation:
An audit report of the controls by the service provider's external auditor provides the best evidence that a third-party service provider's information security controls are effective. An external auditor is an independent and objective party that can assess the design and operating effectiveness of the service provider's information security controls based on established standards and criteria. An external auditor can also provide an opinion on the adequacy and compliance of the service provider's information security controls, as well as recommendations for improvement.
Documentation of the service provider's security configuration controls is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. Documentation of the security configuration controls can show the settings and parameters of the service provider's information systems and networks, but it may not reflect the actual implementation and operation of the controls. Documentation of the security configuration controls may also be outdated, incomplete, or inaccurate.
An interview with the service provider's information security officer is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. An interview with the information security officer can provide insights into the service provider's information security strategy, policies, and procedures, but it may not verify the actual performance and compliance of the information security controls. An interview with the information security officer may also be biased, subjective, or misleading.
A review of the service provider's policies and procedures is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. A review of the policies and procedures can show the service provider's information security objectives, requirements, and guidelines, but it may not demonstrate the actual execution and enforcement of the information security controls. A review of the policies and procedures may also be insufficient, inconsistent, or outdated.
ISACA, CISA Review Manual, 27th Edition, 2019, p. 284
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 111
Which of the following is the MOST effective way to identify exfiltration of sensitive data by a malicious insider?

A. Implement data loss prevention (DLP) software
B. Review perimeter firewall logs
C. Provide ongoing information security awareness training
D. Establish behavioral analytics monitoring

Correct Answer: D
Section:
Explanation:
The most effective way to identify exfiltration of sensitive data by a malicious insider is to establish behavioral analytics monitoring. Behavioral analytics is the process of analyzing the patterns and anomalies in user behavior to detect and prevent insider threats. Behavioral analytics can help identify unusual or suspicious activities, such as accessing sensitive data at odd hours, transferring large amounts of data to external devices or locations, or using unauthorized applications or protocols. Behavioral analytics can also help correlate data from multiple sources, such as network logs, user profiles, and access rights, to provide a holistic view of user activity and risk.
Data loss prevention (DLP) software is a tool that can help prevent exfiltration of sensitive data by a malicious insider, but it is not the most effective way to identify it. DLP software can block or alert on unauthorized data transfers based on predefined rules and policies, but it may not be able to detect sophisticated or stealthy exfiltration techniques, such as encryption, steganography, or data obfuscation.
Reviewing perimeter firewall logs is a way to identify exfiltration of sensitive data by a malicious insider, but it is not the most effective way. Perimeter firewall logs can show the traffic volume and destination of data transfers, but they may not be able to show the content or context of the data. Perimeter firewall logs may also be overwhelmed by the amount of normal traffic and miss the signals of malicious exfiltration.
Providing ongoing information security awareness training is a way to reduce the risk of exfiltration of sensitive data by a malicious insider, but it is not a way to identify it. Information security awareness training can help educate users on the importance of protecting sensitive data and the consequences of violating policies and regulations, but it may not deter or detect those who are intentionally or maliciously exfiltrating data.
ISACA, CISA Review Manual, 27th Edition, 2019, p. 300
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription1
Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog2

How to Secure Your Company's Legacy Applications - iCorps

QUESTION 112
An IS auditor identifies that a legacy application to be decommissioned in three months cannot meet the security requirements established by the current policy. What is the BEST way (or the auditor to address this issue?

A. Recommend the application be patched to meet requirements.
B. Inform the IT director of the policy noncompliance.
C. Verify management has approved a policy exception to accept the risk.
D. Take no action since the application will be decommissioned in three months.

Correct Answer: C
Section:
Explanation:
The best way for the auditor to address this issue is to verify management has approved a policy exception to accept the risk. A policy exception is a formal authorization that allows a deviation from the established policy requirements for a specific situation or period of time. A policy exception should be based on a risk assessment that evaluates the impact and likelihood of the potential threats and vulnerabilities, as well as the cost and benefit of the alternative controls. A policy exception should also be documented, approved, and monitored by management.
Recommending the application be patched to meet requirements is not the best way for the auditor to address this issue. Patching the application may not be feasible, cost-effective, or timely, given that the application will be decommissioned in three months. Patching the application may also introduce new risks or errors that could affect the functionality or performance of the application.
Informing the IT director of the policy noncompliance is not the best way for the auditor to address this issue. Informing the IT director of the policy noncompliance may not resolve the issue or mitigate the risk, especially if the IT director is already aware of the situation and has decided to accept it. Informing the IT director of the policy noncompliance may also create unnecessary conflict or tension between the auditor and the auditee.
Taking no action since the application will be decommissioned in three months is not the best way for the auditor to address this issue. Taking no action may expose the organization to significant risks or consequences, such as data breaches, regulatory fines, or reputational damage, if the application is compromised or exploited by malicious actors. Taking no action may also violate the auditor's professional standards and responsibilities, such as due care, objectivity, and reporting.
ISACA, CISA Review Manual, 27th Edition, 2019, p. 289
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog
How to Secure Your Company's Legacy Applications - iCorps

QUESTION 113
An IS auditor reviewing the throat assessment for a data cantor would be MOST concerned if:

A. some of the identified threats are unlikely to occur.
B. all identified threats relate to external entities.
C. the exercise was completed by local management.
D. neighboring organizations' operations have been included.

Correct Answer: B
Section:
Explanation:
: An IS auditor reviewing the threat assessment for a data center would be most concerned if all identified threats relate to external entities. This indicates that the threat assessment is incomplete and biased, as it ignores the potential threats from internal sources, such as employees, contractors, vendors, or authorized visitors. Internal threats can pose significant risks to the data center, as they may have access to sensitive information, systems, or facilities, and may exploit their privileges for malicious or fraudulent purposes.According to a study by IBM, 60% of cyberattacks in 2015 were carried out by insiders1
Some of the identified threats are unlikely to occur is not a cause for concern, as it shows that the threat assessment is comprehensive and realistic, and considers all possible scenarios, regardless of their probability. A threat assessment should not exclude any potential threats based on subjective judgments or assumptions, as they may still have a high impact if they materialize.
The exercise was completed by local management is not a cause for concern, as it shows that the threat assessment is conducted by the people who are most familiar with the data center's operations, environment, and risks. Local management may have more relevant and accurate information and insights than external parties, and may be more invested in the outcome of the threat assessment.
Neighboring organizations' operations have been included is not a cause for concern, as it shows that the threat assessment is holistic and contextual, and considers the interdependencies and influences of external factors on the data center's security. Neighboring organizations' operations may pose direct or indirect threats to the data center, such as physical damage, network interference, or shared vulnerabilities.
IBM Security Services 2016 Cyber Security Intelligence Index1

QUESTION 114
Which of the following is the BEST indication of effective IT investment management?

A. IT investments are implemented and monitored following a system development life cycle (SDLC)
B. IT investments are mapped to specific business objectives
C. Key performance indicators (KPIs) are defined for each business requiring IT Investment
D. The IT Investment budget is significantly below industry benchmarks

Correct Answer: B
Section:
Explanation:
This means that the IT investments are aligned with the strategic goals and priorities of the organization, and that they deliver value and benefits to the business. Mapping IT investments to specific business objectives can help ensure that the IT investments are relevant, justified, and measurable, and that they support the organization's mission and vision.
IT investments are implemented and monitored following a system development life cycle (SDLC) is an indication of effective IT project management, but not necessarily of effective IT investment management. The SDLC is a framework that guides the development and implementation of IT systems and applications, but it does not address the alignment, justification, or measurement of the IT investments.
Key performance indicators (KPIs) are defined for each business requiring IT investment is an indication of effective IT performance management, but not necessarily of effective IT investment management. KPIs are metrics that measure the outcomes and results of IT activities and processes, but they do not address the alignment, justification, or value of the IT investments.
The IT investment budget is significantly below industry benchmarks is not an indication of effective IT investment management, but rather of low IT spending. The IT investment budget should be based on the organization's needs and capabilities, and not on external comparisons. A low IT investment budget may indicate that the organization is underinvesting in IT, which could limit its potential for growth and innovation.

QUESTION 115
Which of the following is the MOST important responsibility of user departments associated with program changes?

A. Providing unit test data
B. Analyzing change requests
C. Updating documentation lo reflect latest changes
D. Approving changes before implementation

Correct Answer: D
Section:
Explanation:
The most important responsibility of user departments associated with program changes is approving changes before implementation. This is because user departments are the primary stakeholders and beneficiaries of the program changes, and they need to ensure that the changes meet their requirements, expectations, and objectives. User departments also need to approve the changes before implementation to avoid unauthorized, unnecessary, or erroneous changes that could affect the functionality, performance, or security of the program.
Providing unit test data is a responsibility of user departments associated with program changes, but it is not the most important one. Unit test data is used to verify that the individual components of the program work as expected after the changes. However, unit test data alone cannot guarantee that the program as a whole works correctly, or that the changes are aligned with the user departments' needs.
Analyzing change requests is a responsibility of user departments associated with program changes, but it is not the most important one. Analyzing change requests is the process of evaluating the feasibility, necessity, and impact of the proposed changes. However, analyzing change requests does not ensure that the changes are implemented correctly, or that they are acceptable to the user departments.
Updating documentation to reflect latest changes is a responsibility of user departments associated with program changes, but it is not the most important one. Updating documentation is the process of maintaining accurate and complete records of the program's specifications, features, and functions after the changes. However, updating documentation does not ensure that the changes are effective, or that they are approved by the user departments.
ISACA, CISA Review Manual, 27th Edition, 2019, p. 281
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 116
Audit frameworks cart assist the IS audit function by:

A. defining the authority and responsibility of the IS audit function.

B. providing details on how to execute the audit program.
C. providing direction and information regarding the performance of audits.
D. outlining the specific steps needed to complete audits

Correct Answer: C
Section:
Explanation:
Audit frameworks can assist the IS audit function by providing direction and information regarding the performance of audits. Audit frameworks are sets of standards, guidelines, and best practices that help IS auditors plan, conduct, and report on their audit engagements. Audit frameworks can help IS auditors ensure the quality, consistency, and professionalism of their audit work, as well as comply with the expectations and requirements of the stakeholders and regulators. Audit frameworks can also help IS auditors address the specific challenges and risks of auditing information systems and technology.
Defining the authority and responsibility of the IS audit function is not a way that audit frameworks can assist the IS audit function, but rather a way that the IS audit charter can assist the IS audit function. The IS audit charter is a document that defines the purpose, scope, objectives, and authority of the IS audit function within the organization. The IS audit charter can help IS auditors establish their role and position in relation to other functions and departments, as well as clarify their rights and obligations.
Providing details on how to execute the audit program is not a way that audit frameworks can assist the IS audit function, but rather a way that the audit methodology can assist the IS audit function. The audit methodology is a set of procedures and techniques that guide IS auditors in performing their audit tasks and activities. The audit methodology can help IS auditors apply a systematic and structured approach to their audit work, as well as use appropriate tools and methods to collect and analyze evidence.
Outlining the specific steps needed to complete audits is not a way that audit frameworks can assist the IS audit function, but rather a way that the audit plan can assist the IS audit function. The audit plan is a document that describes the scope, objectives, timeline, resources, and deliverables of a specific audit engagement. The audit plan can help IS auditors organize and manage their audit work, as well as communicate their expectations and responsibilities to the auditees.
ISACA, CISA Review Manual, 27th Edition, 2019, p.511
Understanding Project Audit Frameworks - Wolters Kluwer2
How to Implement a Robust Audit Framework - Insights - Metricstream3
What Is The Internal Audit Function?An Accurate Definition Of The

QUESTION 117
Which of the following would be the BEST process for continuous auditing to a large financial institution?

A. Testing encryption standards on the disaster recovery system
B. Validating access controls for real-time data systems
C. Performing parallel testing between systems
D. Validating performance of help desk metrics

Correct Answer: B
Section:
Explanation:
The best process for continuous auditing for a large financial institution is validating access controls for real-time data systems. This is because access controls are critical for ensuring the confidentiality, integrity, and availability of the financial data that is processed and transmitted by the real-time data systems. Real-time data systems are systems that provide timely and accurate information to support decision-making and transactions in a dynamic and complex environment. Examples of real-time data systems in the financial sector include payment systems, trading platforms, risk management systems, and fraud detection systems. Continuous auditing of access controls can help detect and prevent unauthorized access, data leakage, data manipulation, or data loss that could compromise the security, reliability, or compliance of the real-time data systems.
Testing encryption standards on the disaster recovery system is not the best process for continuous auditing for a large financial institution. Encryption standards are important for protecting the data stored or transmitted by the disaster recovery system, which is a system that provides backup and recovery capabilities in case of a disruption or disaster. However, testing encryption standards is not a continuous process, but rather a periodic or event-driven process that can be performed as part of the disaster recovery plan testing or validation.
Performing parallel testing between systems is not the best process for continuous auditing for a large financial institution. Parallel testing is a process of comparing the results of two or more systems that perform the same function or task, such as a new system and an old system, or a primary system and a backup system. Parallel testing can help verify the accuracy, consistency, and compatibility of the systems. However, parallel testing is not a continuous process, but rather a temporary or transitional process that can be performed as part of the system implementation or migration.
Validating performance of help desk metrics is not the best process for continuous auditing for a large financial institution. Help desk metrics are indicators that measure the efficiency, effectiveness, and quality of the help desk service, which is a service that provides technical support and assistance to the users of information systems and technology. Help desk metrics can include metrics such as response time, resolution time, customer satisfaction, and service level agreement (SLA) compliance. Validating performance of help desk metrics can help evaluate and improve the help desk service. However, validating performance of help desk metrics is not a continuous auditing process, but rather a continuous monitoring process that can be performed by the help desk management or quality assurance team.

All eyes on: Continuous auditing - KPMG Global1
Internal audit's role at financial institutions: PwC2
The Fed - Supervisory Policy and Guidance Topics - Large Banking ...3
Continuous Audit: Definition, Steps, Advantages and Disadvantages4

QUESTION 118
Which of the following methods will BEST reduce the risk associated with the transition to a new system using technologies that are not compatible with the old system?

A. Parallel changeover
B. Modular changeover
C. Phased operation
D. Pilot operation

Correct Answer: A
Section:
Explanation:
The best method to reduce the risk associated with the transition to a new system using technologies that are not compatible with the old system is parallel changeover. Parallel changeover is a method of system conversion that involves running both the old and the new systems simultaneously for a period of time, until the new system is verified to be working correctly and completely. Parallel changeover can help reduce the risk of data loss, errors, or disruptions that may occur due to the incompatibility of the technologies, as well as provide a backup option in case of failure or malfunction of the new system. Parallel changeover can also help users compare and validate the results of both systems, and facilitate their training and adaptation to the new system.
Modular changeover is a method of system conversion that involves replacing one module or component of the old system with a corresponding module or component of the new system at a time, until the entire system is replaced. Modular changeover can help reduce the complexity and scope of the conversion, as well as minimize the impact on the users and operations. However, modular changeover may not be feasible or effective when the technologies of the old and new systems are not compatible, as it may create integration or interoperability issues among the modules.
Phased operation is a method of system conversion that involves implementing the new system in stages or increments, each with a subset of functions or features, until the entire system is operational. Phased operation can help reduce the risk and cost of implementing a large and complex system, as well as allow for testing and feedback at each stage. However, phased operation may not be suitable or efficient when the technologies of the old and new systems are not compatible, as it may require extensive modifications or adaptations to enable partial functionality.
Pilot operation is a method of system conversion that involves implementing the new system in a limited or controlled environment, such as a department or a location, before rolling it out to the entire organization. Pilot operation can help test and evaluate the performance and usability of the new system, as well as identify and resolve any issues or problems before full-scale implementation. However, pilot operation may not be relevant or reliable when the technologies of the old and new systems are not compatible, as it may not reflect the actual conditions or challenges of operating both systems concurrently.
TRANSITION TO THE NEW SYSTEM - O'Reilly Media1
10 Challenges To Think About When Upgrading From Legacy Systems - Forbes

QUESTION 119
An internal audit team is deciding whether to use an audit management application hosted by a third party in a different country.
What should be the MOST important consideration related to the uploading of payroll audit documentation in the hosted application?

A. Financial regulations affecting the organization
B. Data center physical access controls whore the application is hosted
C. Privacy regulations affecting the organization
D. Per-unit cost charged by the hosting services provider for storage

Correct Answer: C
Section:
Explanation:
This is because privacy regulations are laws or rules that protect the personal information of individuals from unauthorized access, use, disclosure, or transfer by third parties. Payroll audit documentation may contain sensitive and confidential data, such as employee names, salaries, benefits, taxes, deductions, and bank accounts. If the audit management application is hosted by a third party in a different country, the organization may need to comply with the privacy regulations of both its own country and the host country, as well as any international or regional agreements or frameworks that apply. Privacy regulations may impose various requirements and obligations on the organization, such as obtaining consent from the data subjects, implementing appropriate security measures, notifying data breaches, and ensuring data quality and accuracy. Privacy regulations may also grant various rights to the data subjects, such as accessing, correcting, deleting, or transferring their data. Failing to comply with privacy regulations may expose the organization to significant risks and consequences,

such as legal actions, fines, sanctions, reputational damage, or loss of trust.
Some examples of privacy regulations affecting the organization are:
The General Data Protection Regulation (GDPR), which is a comprehensive and strict privacy regulation that applies to any organization that processes personal data of individuals in the European Union (EU) or offers goods or services to them, regardless of where the organization or the data is located1.
The California Consumer Privacy Act (CCPA), which is a broad and influential privacy regulation that applies to any organization that collects personal information of California residents and meets certain thresholds of revenue, data volume, or data sharing2.
The Health Insurance Portability and Accountability Act (HIPAA), which is a sector-specific privacy regulation that applies to any organization that handles protected health information (PHI) of individuals in the United States, such as health care providers, health plans, or health care clearinghouses3.
Therefore, before using an audit management application hosted by a third party in a different country, the internal audit team should conduct a thorough assessment of the privacy regulations affecting the organization and ensure that they have adequate policies, procedures, and controls in place to comply with them.

QUESTION 120
Which of the following findings should be of GREATEST concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization?

A. Insufficient processes to track ownership of each EUC application?
B. Insufficient processes to lest for version control
C. Lack of awareness training for EUC users
D. Lack of defined criteria for EUC applications

Correct Answer: D
Section:
Explanation:
The finding that should be of greatest concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization is the lack of defined criteria for EUC applications. EUC applications are applications that are developed and maintained by end-users, rather than by IT professionals, to support their business functions and processes. Examples of EUC applications include spreadsheets, databases, reports, and scripts. The lack of defined criteria for EUC applications means that the organization does not have clear and consistent standards or guidelines to identify, classify, and manage EUC applications. This can lead to various risks, such as:
Inaccurate or unreliable data and results from EUC applications that are not validated, verified, or tested
Unauthorized or inappropriate access or use of EUC applications that are not secured, controlled, or monitored
Inconsistent or incompatible data and results from EUC applications that are not integrated, documented, or updated
Loss or corruption of data and results from EUC applications that are not backed up, recovered, or archived
Therefore, the IS auditor should be most concerned about the lack of defined criteria for EUC applications, as it can affect the quality, integrity, and availability of the EUC applications and the data they produce.
Insufficient processes to track ownership of each EUC application is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. The ownership of an EUC application refers to the person or group who is responsible for creating, maintaining, and using the EUC application. Insufficient processes to track ownership of each EUC application means that the organization does not have adequate mechanisms or records to identify and communicate who owns each EUC application. This can lead to risks, such as:
Lack of accountability or ownership for the quality and accuracy of the EUC application and its data
Lack of support or maintenance for the EUC application when the owner leaves or changes roles
Lack of awareness or training for the users of the EUC application on its purpose and functionality
However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
Insufficient processes to test for version control is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Version control is a process that tracks and manages the changes made to an EUC application over time. Insufficient processes to test for version control means that the organization does not have adequate procedures or tools to ensure that the changes made to an EUC application are authorized, documented, and tested. This can lead to risks, such as:
Errors or inconsistencies in the data and results from different versions of the EUC application
Conflicts or confusion among the users of the EUC application on which version is current or correct
Loss or overwrite of data and results from previous versions of the EUC application
However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
Lack of awareness training for EUC users is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Awareness training for EUC users is a process that educates and informs the users of the EUC applications on their roles, responsibilities, and risks. Lack of awareness training for EUC users means that the organization does not have adequate programs or materials to raise the knowledge and skills of the users on how to use and manage the EUC applications effectively and securely. This can lead to risks, such as:
Misuse or abuse of the EUC applications by users who are not aware of their impact or implications

Non-compliance or violation of policies or regulations by users who are not aware of their requirements or expectations
Dissatisfaction or frustration among users who are not aware of their benefits or limitations
However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
End-user computing - Wikipedia1
How to Manage the Risks Associated with End User Computing2
Managing end user computing risks - KPMG UK3

QUESTION 121
What would be an IS auditor's BEST course of action when an auditee is unable to close all audit recommendations by the time of the follow-up audit?

A. Ensure the open issues are retained in the audit results.
B. Terminate the follow-up because open issues are not resolved
C. Recommend compensating controls for open issues.
D. Evaluate the residual risk due to open issues.

Correct Answer: D
Section:
Explanation:
The best course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit is to evaluate the residual risk due to open issues. Residual risk is the risk that remains after the implementation of controls or mitigating actions. Evaluating the residual risk due to open issues can help the IS auditor assess the impact and likelihood of the potential threats and vulnerabilities that have not been addressed by the auditee, as well as the adequacy and effectiveness of the existing controls or mitigating actions. Evaluating the residual risk due to open issues can also help the IS auditor prioritize and communicate the open issues to the auditee and other stakeholders, such as senior management or audit committee, and recommend appropriate actions or escalation procedures.
Ensuring the open issues are retained in the audit results is a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but it is not the best one. Ensuring the open issues are retained in the audit results can help the IS auditor document and report the status and progress of the audit recommendations, as well as provide a basis for future follow-up audits. However, ensuring the open issues are retained in the audit results does not provide an analysis or evaluation of the residual risk due to open issues, which is more important for informing decision-making and action-taking.
Terminating the follow-up because open issues are not resolved is not a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but rather a consequence or outcome of it. Terminating the follow-up because open issues are not resolved may indicate that the auditee has failed to comply with the agreed-upon actions or deadlines, or that the IS auditor has encountered significant obstacles or resistance from the auditee. Terminating the follow-up because open issues are not resolved may also trigger further actions or sanctions from the IS auditor or other authorities, such as issuing a qualified or adverse opinion, withholding certification, or imposing penalties.
Recommending compensating controls for open issues is not a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but rather a possible outcome or result of it. Compensating controls are alternative or additional controls that are implemented to reduce or eliminate the risk associated with a weakness or deficiency in another control. Recommending compensating controls for open issues may be appropriate when the auditee is unable to implement the original audit recommendations due to technical, operational, financial, or other constraints, and when the compensating controls can provide a similar or equivalent level of assurance. However, recommending compensating controls for open issues requires a prior evaluation of the residual risk due to open issues, which is more important for determining whether compensating controls are necessary and feasible.
Follow-up Audits - Canadian Audit and Accountability Foundation1
Conducting The Audit Follow-Up: When To Verify - The Auditor2
Internal Audit Follow Ups: Are They Really Worth The Effort

QUESTION 122
Which of the following is the BEST way to sanitize a hard disk for reuse to ensure the organization's information cannot be accessed?

A. Re-partitioning
B. Degaussing
C. Formatting
D. Data wiping

Correct Answer: D
Section:
Explanation:

The best way to sanitize a hard disk for reuse to ensure the organization's information cannot be accessed is data wiping. Data wiping is a process that overwrites the data on the hard disk with random or meaningless patterns, making it unrecoverable by any software or hardware methods. Data wiping can provide a high level of security and assurance that the organization's information is permanently erased from the hard disk, and that it cannot be accessed by unauthorized parties or malicious actors.
Re-partitioning is not a way to sanitize a hard disk for reuse, but rather a way to organize the hard disk into different logical sections or volumes. Re-partitioning does not erase the data on the hard disk, but only changes the structure and allocation of the disk space. Re-partitioning may make the data inaccessible to the operating system, but not to other tools or methods that can scan or recover the data from the disk sectors.
Degaussing is a way to sanitize a hard disk for reuse, but only for magnetic hard disks, not solid state drives (SSDs). Degaussing is a process that exposes the hard disk to a strong magnetic field, which disrupts and destroys the magnetic alignment of the data on the disk platters. Degaussing can effectively erase the data on magnetic hard disks, but it can also damage or render unusable the electronic components of the hard disk, such as the read/write heads or circuit boards. Degaussing also does not work on SSDs, which store data using flash memory cells, not magnetic media.
Formatting is not a way to sanitize a hard disk for reuse, but rather a way to prepare the hard disk for use by an operating system. Formatting is a process that creates a file system on the hard disk, which defines how the data is stored and accessed on the disk. Formatting does not erase the data on the hard disk, but only deletes the file system metadata and marks the disk space as available for new data. Formatting may make the data invisible to the operating system, but not to other tools or methods that can restore or recover the data from the disk sectors.
How to Wipe A Hard Drive for Reuse?Check the Quickest Way to Wipe A Hard Drive - EaseUS1
HP PCs - Using Secure Erase or HP Disk Sanitizer2
HOW to QUICKLY and PERMANENTLY SANITIZE ANY DRIVE (SSD, USB thumb drive ...)

QUESTION 123
in a post-implantation Nation review of a recently purchased system it is MOST important for the iS auditor to determine whether the:

A. stakeholder expectations were identified
B. vendor product offered a viable solution.
C. user requirements were met.
D. test scenarios reflected operating activities.

Correct Answer: C
Section:
Explanation:
The most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system is whether the user requirements were met. User requirements are the specifications and expectations of the users of the system, such as the features, functions, performance, quality, and security of the system. User requirements are usually defined and documented in the early stages of the system acquisition process, such as in the request for proposal (RFP) or the contract. User requirements are also used as the basis for testing and evaluating the system before and after implementation.
Determining whether the user requirements were met can help the IS auditor assess whether the system is fit for purpose and delivers value and benefits to the users and the organization. Determining whether the user requirements were met can also help the IS auditor identify any gaps, issues, or problems with the system that may affect its functionality, usability, or reliability. Determining whether the user requirements were met can also help the IS auditor provide feedback and recommendations for improvement or enhancement of the system.
Stakeholder expectations were identified is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather a prerequisite or input for it. Stakeholder expectations are the needs and wants of the various parties who have an interest or influence in the system, such as users, managers, customers, suppliers, regulators, or auditors. Stakeholder expectations are usually identified and analyzed in the initial stages of the system acquisition process, such as in the feasibility study or the business case. Stakeholder expectations are also used as inputs for defining and prioritizing the user requirements.
Test scenarios reflected operating activities is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather a factor or criterion for it. Test scenarios are sets of conditions or situations that are used to test and verify whether the system meets the user requirements. Test scenarios reflected operating activities means that test scenarios simulated or replicated real-world scenarios that occur during normal operations of business processes or functions that use or depend on the system. Test scenarios reflected operating activities can help ensure that test results are valid, reliable, and relevant.
Post Implementation Review: How to conduct and its Benefits1
Post-implementation reviews - Department of Prime Minister and Cabinet2
How To Conduct A Post Implementation Audit of Your Recently Installed System3

QUESTION 124
An IS auditor is evaluating the access controls for a shared customer relationship management (CRM) system. Which of the following would be the GREATEST concern?

A. Single sign-on is not enabled
B. Audit logging is not enabled
C. Security baseline is not consistently applied

D. Complex passwords are not required

Correct Answer: B
Section:
Explanation:
The greatest concern for an IS auditor evaluating the access controls for a shared customer relationship management (CRM) system is that audit logging is not enabled. Audit logging is a process that records and tracks the activities and events that occur on a system, such as who accessed what data, when, how, and why. Audit logging can help monitor and verify the compliance and effectiveness of the access controls, as well as detect and investigate any unauthorized or suspicious access or actions. Audit logging can also provide evidence and accountability for the security and integrity of the system and the data.
Without audit logging, the IS auditor would not be able to audit the access controls for the shared CRM system, as there would be no reliable or traceable records of the access history or patterns. Without audit logging, the organization would also not be able to identify or respond to any potential breaches or incidents that may compromise the confidentiality, availability, or accuracy of the CRM data. Without audit logging, the organization would also not be able to demonstrate or prove its compliance with any applicable policies, regulations, or standards that may require audit logging for CRM systems.
Single sign-on is not enabled is not a great concern for an IS auditor evaluating the access controls for a shared CRM system, but rather a potential improvement or enhancement. Single sign-on is a process that allows users to access multiple systems or applications with one set of credentials, such as a username and password. Single sign-on can help simplify and streamline the user experience, as well as reduce the risk of password fatigue or compromise. However, single sign-on is not a mandatory or essential requirement for access controls, and it may also introduce some challenges or risks, such as dependency on a single point of failure or vulnerability.
Security baseline is not consistently applied is not a great concern for an IS auditor evaluating the access controls for a shared CRM system, but rather a minor issue or gap. Security baseline is a set of minimum security standards or requirements that apply to a system or application, such as password policies, encryption protocols, or firewall rules. Security baseline can help ensure that the system or application meets a certain level of security and compliance. However, security baseline is not a sufficient or comprehensive measure for access controls, and it may also need to be customized or adjusted according to the specific needs and risks of each system or application.
Complex passwords are not required is not a great concern for an IS auditor evaluating the access controls for a shared CRM system, but rather a common practice or recommendation. Complex passwords are passwords that are composed of a combination of different types of characters, such as letters, numbers, symbols, and cases. Complex passwords can help prevent or deter brute-force attacks or guessing attempts by making the passwords harder to crack or predict. However, complex passwords are not a guarantee or guarantee of security, and they may also have some drawbacks or limitations, such as user inconvenience, memorability issues, or reuse across multiple systems or applications.
Customer Relationship Management Risks and Controls - CRM Simplified1
Customer relationship management: A guide - Zendesk2
How to Protect Your Customer Relationship Management (CRM) Data from Hackers3
What is CRM?| A Definition by Salesforce4

QUESTION 125
An IS auditor concludes that logging and monitoring mechanisms within an organization are ineffective because critical servers are not included within the central log repository. Which of the following audit procedures would have MOST likely identified this exception?

A. Inspecting a sample of alerts generated from the central log repository
B. Comparing a list of all servers from the directory server against a list of all servers present in the central log repository
C. Inspecting a sample of alert settings configured in the central log repository
D. Comparing all servers included in the current central log repository with the listing used for the prior-year audit

Correct Answer: B
Section:
Explanation:
The audit procedure that would have most likely identified the exception of critical servers not included in the central log repository is to compare a list of all servers from the directory server against a list of all servers present in the central log repository. This would allow the IS auditor to detect any discrepancies or omissions in the central log repository. The other audit procedures (A, C and D) would not be effective in identifying this exception, as they would only focus on the alerts generated, the alert settings configured, or the servers included in the previous year's audit, which may not reflect the current state of the central log repository.Reference:IS Audit and Assurance Guideline 2202: Evidence Collection Techniques,CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.3: Logging and Monitoring

QUESTION 126
A financial group recently implemented new technologies and processes, Which type of IS audit would provide the GREATEST level of assurance that the department's objectives have been met?

A. Performance audit
B. Integrated audit

C. Cyber audit
D. Financial audit

Correct Answer: B
Section:
Explanation:
The type of IS audit that would provide the greatest level of assurance that the department's objectives have been met after implementing new technologies and processes is an integrated audit. An integrated audit is an audit that combines financial, operational, compliance, and IT auditing aspects to provide a holistic view of the organization's performance and risks. An integrated audit can evaluate whether the new technologies and processes are aligned with the organization's goals, strategies, policies, and controls, and whether they are delivering value, efficiency, effectiveness, and reliability. The other types of IS audits (A, C and D) would not provide the same level of assurance, as they would only focus on specific aspects of the organization's activities, such as performance, cyber security, or financial reporting, which may not capture the full impact of the new technologies and processes.Reference:CISA Certification | Certified Information Systems Auditor | ISACA,CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.2: Types of IS Audit Engagements

QUESTION 127
Which of the following areas is MOST likely to be overlooked when implementing a new data classification process?

A. End-user computing (EUC) systems
B. Email attachments
C. Data sent to vendors
D. New system applications

Correct Answer: A
Section:
Explanation:
The area that is most likely to be overlooked when implementing a new data classification process is end-user computing (EUC) systems. EUC systems are applications or tools that are developed or customized by end users, often without formal IT involvement or approval. EUC systems may contain sensitive or confidential data that need to be classified and protected according to the organization's policies and standards. However, EUC systems may not be subject to the same controls, oversight, or documentation as formal IT systems, and may not be included in the scope of the data classification process. Therefore, EUC systems pose a significant risk of data leakage, unauthorized access, or noncompliance. The other areas (B, C and D) are less likely to be overlooked, as they are more visible and manageable by the IT department or the data owners.Reference:IS Audit and Assurance Guideline 2202: Evidence Collection Techniques,CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.2: Data Classification

QUESTION 128
An IS auditor Is renewing the deployment of a new automated system Which of the following findings presents the MOST significant risk?

A. The new system has resulted m layoffs of key experienced personnel.
B. Users have not been trained on the new system.
C. Data from the legacy system is not migrated correctly to the new system.
D. The new system is not platform agnostic

Correct Answer: C
Section:
Explanation:
The finding that presents the most significant risk when reviewing the deployment of a new automated system is that data from the legacy system is not migrated correctly to the new system. Data migration is a critical process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. If data migration is not performed correctly, it can result in data loss, corruption, inconsistency, or duplication, which can affect the functionality, performance, reliability, and security of the new system. Data migration errors can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The other findings (A, B and D) are less significant risks, as they can be mitigated by rehiring or retraining personnel, providing user training, or adapting the system to different platforms.

QUESTION 129

Which of the following is an advantage of using agile software development methodology over the waterfall methodology?

A. Less funding required overall
B. Quicker deliverables
C. Quicker end user acceptance
D. Clearly defined business expectations

Correct Answer: B
Section:
Explanation:
The advantage of using agile software development methodology over the waterfall methodology is that it allows for quicker deliverables. Agile software development is an iterative and incremental approach that emphasizes customer feedback, collaboration, and adaptation. Agile software development delivers working software in short cycles, called sprints, that typically last from two to four weeks. This enables the development team to respond to changing requirements, deliver value faster, and improve quality. Waterfall software development is a linear and sequential approach that follows a predefined set of phases, such as planning, analysis, design, implementation, testing, and maintenance. Waterfall software development requires a clear and stable definition of the project scope, deliverables, and expectations before starting the development process. Waterfall software development can be slow, rigid, and costly, especially if changes occur during the later stages of the project.Reference:CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.1: Project Management Practices

QUESTION 130
Which of the following is the BEST control to minimize the risk of unauthorized access to lost company-owned mobile devices?

A. Password/PIN protection
B. Device tracking software
C. Device encryption
D. Periodic backup

Correct Answer: C
Section:
Explanation:
The best control to minimize the risk of unauthorized access to lost company-owned mobile devices is device encryption. Device encryption is a process that transforms data on a device into an unreadable format using a cryptographic key. Device encryption protects the data stored on the device from being accessed by unauthorized parties, even if they bypass the password or PIN protection. Device encryption can also prevent data leakage if the device is disposed of or recycled without proper data sanitization. Password or PIN protection is a basic control that prevents unauthorized access to the device by requiring a secret code or pattern to unlock it. However, password or PIN protection can be easily compromised by brute force attacks, shoulder surfing, or social engineering. Device tracking software is a tool that allows the device owner or administrator to locate, lock, or wipe the device remotely in case of loss or theft. However, device tracking software depends on the device's network connectivity and GPS functionality, which may not be available or reliable in some situations. Periodic backup is a process that copies the data from the device to another storage location for recovery purposes. Periodic backup can help restore the data in case of loss or damage of the device, but it does not prevent unauthorized access to the data on the device itself.Reference:CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Mobile Devices

QUESTION 131
Which of the following is the BEST approach for determining the overall IT risk appetite of an organization when business units use different methods for managing IT risks?

A. Average the business units' IT risk levels
B. Identify the highest-rated IT risk level among the business units
C. Prioritize the organization's IT risk scenarios
D. Establish a global IT risk scoring criteria

Correct Answer: C
Section:
Explanation:
The best approach for determining the overall IT risk appetite of an organization when business units use different methods for managing IT risks is to prioritize the organization's IT risk scenarios. IT risk appetite is the amount

and type of IT risk that an organization is willing to accept in pursuit of its objectives. IT risk scenarios are hypothetical situations that describe the potential impact of IT risk events on the organization's objectives, processes, and resources. By prioritizing the organization's IT risk scenarios, the IS auditor can identify the most significant IT risks that affect the organization as a whole, and align them with the organization's strategic goals, values, and culture. Prioritizing the organization's IT risk scenarios can also help to communicate and monitor the IT risk appetite across the organization, and facilitate consistent and informed decision making. The other approaches (A, B and D) are not effective for determining the overall IT risk appetite of an organization, as they do not consider the impact and likelihood of IT risks on the organization's objectives, nor do they account for the diversity and complexity of IT risks across different business units.Reference:CISA Review Manual (Digital Version), Chapter 2: Governance and Management of Information Technology, Section 2.3: Information Technology Risk Management

QUESTION 132
Which of the following should be of GREATEST concern to an |$ auditor reviewing data conversion and migration during the implementation of a new application system?

A. The change management process was not formally documented
B. Backups of the old system and data are not available online
C. Unauthorized data modifications occurred during conversion,
D. Data conversion was performed using manual processes

Correct Answer: C
Section:
Explanation:
The finding that should be of greatest concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system is that unauthorized data modifications occurred during conversion. Data conversion and migration is a process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. Unauthorized data modifications during conversion can result in data loss, corruption, inconsistency, or duplication, which can affect the functionality, performance, reliability, and security of the new system. Unauthorized data modifications can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The IS auditor should verify that adequate controls are in place to prevent, detect, and correct unauthorized data modifications during conversion, such as access control, data validation, reconciliation, audit trail, and backup and recovery. The other findings (A, B and D) are less concerning, as they can be mitigated by documenting the change management process, restoring the backups of the old system and data from offline storage, or automating the data conversion process.Reference:CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.4: System Implementation

QUESTION 133
An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported. The auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

A. Verify all patches have been applied to the software system's outdated version.
B. Close all unused ports on the outdated software system.
C. Monitor network traffic attempting to reach the outdated software system.
D. Segregate the outdated software system from the main network.

Correct Answer: D
Section:
Explanation:
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. This will limit the exposure of the system to potential attacks and prevent it from compromising other systems on the network. Segregating the system will also reduce the impact of any security incidents that may occur on the system.
Monitoring network traffic attempting to reach the outdated software system (option C) is not the best way to reduce the risk, as it will not prevent or stop any attacks on the system. It will only provide visibility into the network activity and alert the auditee of any suspicious or malicious traffic.
Verifying all patches have been applied to the software system's outdated version (option A) and closing all unused ports on the outdated software system (option B) are also not the best ways to reduce the risk, as they will not address the underlying issue of using an unsupported version of the software. Patches and ports may still have vulnerabilities that are not fixed by the vendor, and attackers may exploit them to gain access to the system.
Therefore, option D is the correct answer.
Introduction (Part 1 of 7: Mitigating Risks of Unsupported Operating Systems)
Summary (Part 7 of 7: Mitigating Risks of Unsupported Operating Systems)
Upgrade, Retire, or Replace Unsupported Software (Part 4 of 7: Mitigating Risks of Unsupported Operating Systems)

QUESTION 134
An IS auditor finds that while an organization's IT strategy is heavily focused on research and development, the majority of protects n the IT portfolio focus on operations and maintenance. Which of the Mowing is the BEST recommendation?

A. Align the IT strategy will business objectives
B. Review priorities in the IT portfolio
C. Change the IT strategy to focus on operational excellence.
D. Align the IT portfolio with the IT strategy.

Correct Answer: A
Section:
Explanation:
The best recommendation is to align the IT strategy with the business objectives. This will ensure that the IT projects and initiatives are consistent with the organization's vision, mission, and goals. IT strategy should be derived from and support the business strategy, not the other way around. By aligning the IT strategy with the business objectives, the organization can achieve better value, performance, and alignment from its IT investments.
Reviewing priorities in the IT portfolio (option B) is not the best recommendation, as it does not address the root cause of the misalignment between the IT strategy and the IT portfolio. The IT portfolio should reflect the IT strategy, which in turn should reflect the business objectives. Simply changing the priorities in the IT portfolio without aligning the IT strategy with the business objectives may result in suboptimal or conflicting outcomes.
Changing the IT strategy to focus on operational excellence (option C) is also not the best recommendation, as it may not be aligned with the business objectives. The organization's IT strategy should be based on its competitive advantage, market position, customer needs, and industry trends. If the organization's business strategy is heavily focused on research and development, then changing the IT strategy to focus on operational excellence may not be appropriate or beneficial.
Aligning the IT portfolio with the IT strategy (option D) is also not the best recommendation, as it does not address the misalignment between the IT strategy and the business objectives. Aligning the IT portfolio with the IT strategy may improve the coherence and consistency of the IT projects, but it may not ensure that they are aligned with the organization's vision, mission, and goals.
Therefore, option A is the correct answer.
The Challenges of Aligning IT and the Business | CIO Insight
Strategic alignment and value maximization for IT project portfolios ...
A Guide to IT Portfolio Management | Adobe Workfront

QUESTION 135
Which of the following is the BEST performance indicator for the effectiveness of an incident management program?

A. Average time between incidents
B. Incident alert meantime
C. Number of incidents reported
D. Incident resolution meantime

Correct Answer: D
Section:
Explanation:
The best performance indicator for the effectiveness of an incident management program is the incident resolution meantime. This is the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. The incident resolution meantime reflects how quickly and efficiently the incident management team can restore normal service and minimize the impact of incidents on the business operations and customer satisfaction.
The average time between incidents (option A) is not a good performance indicator for the effectiveness of an incident management program, as it does not measure how well the incidents are handled or resolved. It only shows how frequently the incidents occur, which may depend on various factors beyond the control of the incident management team, such as the complexity and reliability of the systems, the security threats and vulnerabilities, and the user behavior and expectations.
The incident alert meantime (option B) is the average time it takes to detect and report an incident. While this is an important metric for measuring the responsiveness and awareness of the incident management team, it does not indicate how effective the incident management program is in resolving the incidents and restoring normal service.
The number of incidents reported (option C) is also not a good performance indicator for the effectiveness of an incident management program, as it does not reflect how well the incidents are handled or resolved. It only shows how many incidents are identified and recorded, which may vary depending on the reporting channels, tools, and procedures used by the incident management team and the users.
Therefore, option D is the correct answer.

Incident Management: Processes, Best Practices & Tools - Atlassian
What is backup and disaster recovery? | IBM

QUESTION 136
Which of the following is the BEST way to verify the effectiveness of a data restoration process?

A. Performing periodic reviews of physical access to backup media
B. Performing periodic complete data restorations
C. Validating off ne backups using software utilities
D. Reviewing and updating data restoration policies annually

Correct Answer: B
Section:
Explanation:
The best way to verify the effectiveness of a data restoration process is to perform periodic complete data restorations. This is the process of transferring backup data to the primary system or data center and verifying that the restored data is accurate, complete, and functional. By performing periodic complete data restorations, the auditee can test the reliability and validity of the backup data, the functionality and performance of the restoration tools and procedures, and the compatibility and integrity of the restored data with the primary system. This will also help identify and resolve any issues or errors that may occur during the restoration process, such as corrupted or missing files, incompatible formats, or configuration problems.
Performing periodic reviews of physical access to backup media (option A) is not the best way to verify the effectiveness of a data restoration process, as it only ensures the security and availability of the backup media, not the quality or usability of the backup data. Physical access reviews are important for preventing unauthorized access, theft, damage, or loss of backup media, but they do not test the actual restoration process or verify that the backup data can be successfully restored.
Validating offline backups using software utilities (option C) is also not the best way to verify the effectiveness of a data restoration process, as it only checks the integrity and consistency of the backup data, not the functionality or compatibility of the restored data. Software utilities can help detect and correct any errors or inconsistencies in the backup data, such as checksum errors, duplicate files, or incomplete backups, but they do not test the actual restoration process or verify that the restored data can work with the primary system.
Reviewing and updating data restoration policies annually (option D) is also not the best way to verify the effectiveness of a data restoration process, as it only ensures that the policies are current and relevant, not that they are implemented and followed. Data restoration policies are important for defining roles and responsibilities, objectives and scope, standards and procedures, and metrics and reporting for the restoration process, but they do not test the actual restoration process or verify that it meets the expected outcomes.
Therefore, option B is the correct answer.
What is backup and disaster recovery? | IBM
Backup and Recovery of Data: The Essential Guide | Veritas
Database Backup and Recovery Best Practices - ISACA

QUESTION 137
In which phase of the internal audit process is contact established with the individuals responsible for the business processes in scope for review?

A. Planning phase
B. Execution phase
C. Follow-up phase
D. Selection phase

Correct Answer: A
Section:
Explanation:
The planning phase is the stage of the internal audit process where contact is established with the individuals responsible for the business processes in scope for review. The planning phase involves defining the objectives, scope, and criteria of the audit, as well as identifying the key risks and controls related to the audited area. The planning phase also involves communicating with the auditee to obtain relevant information, documents, and data, as well as to schedule interviews, walkthroughs, and meetings. The planning phase aims to ensure that the audit team has a clear understanding of the audited area and its context, and that the audit plan is aligned with the expectations and needs of the auditee and other stakeholders.
The execution phase is the stage of the internal audit process where the audit team performs the audit procedures according to the audit plan. The execution phase involves testing the design and operating effectiveness of the controls, collecting and analyzing evidence, documenting the audit work and results, and identifying any issues or findings. The execution phase aims to provide sufficient and appropriate evidence to support the audit

conclusions and recommendations.
The follow-up phase is the stage of the internal audit process where the audit team monitors and verifies the implementation of the corrective actions agreed upon by the auditee in response to the audit findings. The follow-up phase involves reviewing the evidence provided by the auditee, conducting additional tests or interviews if necessary, and evaluating whether the corrective actions have adequately addressed the root causes of the findings. The follow-up phase aims to ensure that the auditee has taken timely and effective actions to improve its processes and controls.
The selection phase is not a standard stage of the internal audit process, but it may refer to the process of selecting which areas or functions to audit based on a risk assessment or an annual audit plan. The selection phase involves evaluating the inherent and residual risks of each potential auditable area, considering the impact, likelihood, and frequency of those risks, as well as other factors such as regulatory requirements, stakeholder expectations, previous audit results, and available resources. The selection phase aims to prioritize and allocate the audit resources to those areas that present the highest risks or opportunities for improvement.
Therefore, option A is the correct answer.
Stages and phases of internal audit - piranirisk.com
Step-by-Step Internal Audit Checklist | AuditBoard
Audit Process | The Office of Internal Audit - University of Oregon

QUESTION 138
A bank has a combination of corporate customer accounts (higher monetary value) and small business accounts (lower monetary value) as part of online banking. Which of the following is the BEST sampling approach for an IS auditor to use for these accounts?

A. Difference estimation sampling
B. Stratified mean per unit sampling
C. Customer unit sampling
D. Unstratified mean per unit sampling

Correct Answer: B
Section:
Explanation:
Stratified mean per unit sampling is a method of audit sampling that divides the population into subgroups (strata) based on some characteristic, such as monetary value, and then selects a sample from each stratum using mean per unit sampling. Mean per unit sampling is a method of audit sampling that estimates the total value of a population by multiplying the average value of the sample items by the number of items in the population. Stratified mean per unit sampling is suitable for populations that have a high variability or a skewed distribution, such as the bank accounts in this question. By stratifying the population, the auditor can reduce the sampling error and increase the precision of the estimate.
Difference estimation sampling (option A) is not the best sampling approach for these accounts. Difference estimation sampling is a method of audit sampling that estimates the total error or misstatement in a population by multiplying the average difference between the book value and the audited value of the sample items by the number of items in the population. Difference estimation sampling is suitable for populations that have a low variability and a symmetrical distribution, which is not the case for the bank accounts in this question.
Customer unit sampling (option C) is not a sampling approach, but a type of monetary unit sampling. Monetary unit sampling is a method of audit sampling that selects sample items based on their monetary value, rather than their physical units. Customer unit sampling is a variation of monetary unit sampling that treats each customer account as a single unit, regardless of how many transactions or balances it contains. Customer unit sampling may be appropriate for testing existence or occurrence assertions, but not for estimating total values.
Unstratified mean per unit sampling (option D) is not the best sampling approach for these accounts. Unstratified mean per unit sampling is a method of audit sampling that applies mean per unit sampling to the entire population without dividing it into subgroups. Unstratified mean per unit sampling may result in a larger sample size and a lower precision than stratified mean per unit sampling, especially for populations that have a high variability or a skewed distribution, such as the bank accounts in this question.
Therefore, option B is the correct answer.
Audit Sampling - AICPA
Audit Sampling: Examples and Guidance To The Sampling Methods
Audit Sampling | Audit | Financial Audit - Scribd

QUESTION 139
Which of the following should be the FIRST step to successfully implement a corporate data classification program?

A. Approve a data classification policy.
B. Select a data loss prevention (DLP) product.
C. Confirm that adequate resources are available for the project.
D. Check for the required regulatory requirements.

Correct Answer: A
Section:
Explanation:
The first step to successfully implement a corporate data classification program is to approve a data classification policy. A data classification policy is a document that defines the objectives, scope, principles, roles, responsibilities, and procedures for classifying data based on its sensitivity and value to the organization. A data classification policy is essential for establishing a common understanding and a consistent approach for data classification across the organization, as well as for ensuring compliance with relevant regulatory and contractual requirements.
Selecting a data loss prevention (DLP) product (option B) is not the first step to implement a data classification program, as it is a technical solution that supports the enforcement of the data classification policy, not the definition of it. A DLP product can help prevent unauthorized access, use, or disclosure of sensitive data by monitoring, detecting, and blocking data flows that violate the data classification policy. However, before selecting a DLP product, the organization needs to have a clear and approved data classification policy that specifies the criteria and rules for data classification.
Confirming that adequate resources are available for the project (option C) is also not the first step to implement a data classification program, as it is a project management activity that ensures the feasibility and sustainability of the project, not the design of it. Confirming that adequate resources are available for the project involves estimating and securing the necessary budget, staff, time, and tools for implementing and maintaining the data classification program. However, before confirming that adequate resources are available for the project, the organization needs to have a clear and approved data classification policy that defines the scope and objectives of the project.
Checking for the required regulatory requirements (option D) is also not the first step to implement a data classification program, as it is an input to the development of the data classification policy, not an output of it. Checking for the required regulatory requirements involves identifying and analyzing the applicable laws, regulations, standards, and contracts that govern the protection and handling of sensitive data. However, checking for the required regulatory requirements is not enough to implement a data classification program; the organization also needs to have a clear and approved data classification policy that incorporates and complies with those requirements.
Therefore, option A is the correct answer.
Data Classification: What It Is and How to Implement It
Create a well-designed data classification framework
7 Steps to Effective Data Classification | CDW
Data Classification: The Basics and a 6-Step Checklist - NetApp
Private and confidential February 2021 - Deloitte US

QUESTION 140
A CFO has requested an audit of IT capacity management due to a series of finance system slowdowns during month-end reporting. What would be MOST important to consider before including this audit in the program?

A. Whether system delays result in more frequent use of manual processing
B. Whether the system's performance poses a significant risk to the organization
C. Whether stakeholders are committed to assisting with the audit
D. Whether internal auditors have the required skills to perform the audit

Correct Answer: B
Section:
Explanation:
The most important thing to consider before including an audit of IT capacity management in the program is whether the system's performance poses a significant risk to the organization. IT capacity management is a process that ensures that IT resources are sufficient to meet current and future business needs, and that they are optimized for cost and performance. A poor IT capacity management can result in system slowdowns, outages, failures, or breaches, which can affect the availability, reliability, security, and efficiency of IT services and business processes. Therefore, before conducting an audit of IT capacity management, the auditor should assess the potential impact and likelihood of these risks on the organization's objectives, reputation, compliance, and customer satisfaction.
Whether system delays result in more frequent use of manual processing (option A) is not the most important thing to consider before including an audit of IT capacity management in the program, as it is only one possible consequence of poor IT capacity management. Manual processing can introduce errors, delays, inefficiencies, and inconsistencies in the data and reports, which can affect the quality and accuracy of financial information. However, manual processing is not the only or the worst outcome of poor IT capacity management; there may be other more severe or frequent risks that need to be considered.
Whether stakeholders are committed to assisting with the audit (option C) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the feasibility and effectiveness of the audit, not the necessity or priority of it. Stakeholder commitment is important for ensuring that the auditor has access to relevant information, documents, data, and personnel, as well as for facilitating communication, collaboration, and feedback during the audit process. However, stakeholder commitment is not a sufficient reason to conduct an audit of IT capacity management; there must be a clear risk-based rationale for selecting this area for audit.
Whether internal auditors have the required skills to perform the audit (option D) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the quality and credibility of the audit, not the urgency or importance of it. Internal auditors should have the appropriate knowledge, skills, and experience to perform an audit of IT capacity management, which may include technical, business, analytical, and communication skills. However, internal auditors can also acquire or supplement these skills through training, coaching, consulting, or outsourcing. Therefore, internal auditors' skills

are not a decisive factor for choosing this area for audit.
Therefore, option B is the correct answer.
Guide to IT Capacity Management | Smartsheet
ISO 27001 capacity management: How to implement control A.12.1.3 - Advisera
ISO 27002:2022 -- Control 8.6 -- Capacity Management

QUESTION 141
The use of which of the following is an inherent risk in the application container infrastructure?

A. Shared registries
B. Host operating system
C. Shared data
D. Shared kernel

Correct Answer: D
Section:
Explanation:
Application containers are a form of operating system virtualization that share the same kernel as the host operating system. This means that any vulnerability or compromise in the kernel can affect all the containers running on the same host, as well as the host itself. Additionally, containers may have privileged access to the kernel resources and functions, which can pose a risk of unauthorized or malicious actions by the container processes. Therefore, securing the kernel is a critical aspect of application container security.
Shared registries (option A) are not an inherent risk in the application container infrastructure, but they are a potential risk that depends on how they are configured and managed. Shared registries are repositories that store and distribute container images. They can be public or private, and they can have different levels of security and access controls. Shared registries can pose a risk of exposing sensitive data, distributing malicious or vulnerable images, or allowing unauthorized access to images. However, these risks can be mitigated by using secure connections, authentication and authorization mechanisms, image signing and scanning, and encryption.
Host operating system (option B) is not an inherent risk in the application container infrastructure, but it is a potential risk that depends on how it is configured and maintained. Host operating system is the underlying platform that runs the application containers and provides them with the necessary resources and services. Host operating system can pose a risk of exposing vulnerabilities, misconfigurations, or malware that can affect the containers or the host itself. However, these risks can be mitigated by using minimal and hardened operating systems, applying patches and updates, enforcing security policies and controls, and isolating and monitoring the host.
Shared data (option C) is not an inherent risk in the application container infrastructure, but it is a potential risk that depends on how it is stored and accessed. Shared data is the information that is used or generated by the application containers and that may be shared among them or with external entities. Shared data can pose a risk of leaking confidential or sensitive data, corrupting or losing data integrity, or violating data privacy or compliance requirements. However, these risks can be mitigated by using secure storage solutions, encryption and decryption mechanisms, access control and auditing policies, and backup and recovery procedures.
Therefore, option D is the correct answer.
Application Container Security Guide | NIST
CSA for a Secure Application Container Architecture
Application Container Security: Risks and Countermeasures

QUESTION 142
A data center's physical access log system captures each visitor's identification document numbers along with the visitor's photo. Which of the following sampling methods would be MOST useful to an IS auditor conducting compliance testing for the effectiveness of the system?

A. Quota sampling
B. Haphazard sampling
C. Attribute sampling
D. Variable sampling

Correct Answer: C
Section:
Explanation:
Attribute sampling is a method of audit sampling that is used to test the effectiveness of controls by measuring the rate of deviation from a prescribed procedure or attribute. Attribute sampling is suitable for testing compliance with the data center's physical access log system, as the auditor can compare the identification document numbers and photos of the visitors with the records in the system and determine whether there are any

discrepancies or errors. Attribute sampling can also provide an estimate of the deviation rate in the population and allow the auditor to draw a conclusion about the operating effectiveness of the control.
Variable sampling, on the other hand, is a method of audit sampling that is used to estimate the amount or value of a population by measuring a characteristic of interest, such as monetary value, quantity, or size. Variable sampling is not appropriate for testing compliance with the data center's physical access log system, as the auditor is not interested in estimating the value of the population, but rather in testing whether the system is operating as intended.
Quota sampling and haphazard sampling are both examples of non-statistical sampling methods that do not use probability theory to select a sample. Quota sampling involves selecting a sample based on certain criteria or quotas, such as age, gender, or location. Haphazard sampling involves selecting a sample without any specific plan or method. Both methods are not suitable for testing compliance with the data center's physical access log system, as they do not ensure that the sample is representative of the population and do not allow the auditor to measure the sampling risk or project the results to the population.
Therefore, attribute sampling is the most useful sampling method for an IS auditor conducting compliance testing for the effectiveness of the data center's physical access log system.
Audit Sampling - What Is It, Methods, Example, Advantage, Reason
ISA 530: Audit sampling | ICAEW

QUESTION 143
Which of the following is the MOST appropriate indicator of change management effectiveness?

A. Time lag between changes to the configuration and the update of records
B. Number of system software changes
C. Time lag between changes and updates of documentation materials
D. Number of incidents resulting from changes

Correct Answer: D
Section:
Explanation:
Change management is the process of planning, implementing, monitoring, and evaluating changes to an organization's information systems and related components. Change management aims to ensure that changes are aligned with the business objectives, minimize risks and disruptions, and maximize benefits and value.
One of the key aspects of change management is measuring its effectiveness, which means assessing whether the changes have achieved the desired outcomes and met the expectations of the stakeholders. There are various indicators that can be used to measure change management effectiveness, such as time, cost, quality, scope, satisfaction, and performance.
Among the four options given, the most appropriate indicator of change management effectiveness is the number of incidents resulting from changes. An incident is an unplanned event or interruption that affects the normal operation or service delivery of an information system. Incidents can be caused by various factors, such as errors, defects, failures, malfunctions, or malicious attacks. Incidents can have negative impacts on the organization, such as loss of data, productivity, reputation, or revenue.
The number of incidents resulting from changes is a direct measure of how well the changes have been planned, implemented, monitored, and evaluated. A high number of incidents indicates that the changes have not been properly tested, verified, communicated, or controlled. A low number of incidents indicates that the changes have been executed smoothly and successfully. Therefore, the number of incidents resulting from changes reflects the quality and effectiveness of the change management process.
The other three options are not as appropriate indicators of change management effectiveness as the number of incidents resulting from changes. The time lag between changes to the configuration and the update of records is a measure of how timely and accurate the configuration management process is. Configuration management is a subset of change management that focuses on identifying, documenting, and controlling the configuration items (CIs) that make up an information system. The time lag between changes and updates of documentation materials is a measure of how well the documentation process is aligned with the change management process. Documentation is an important aspect of change management that provides information and guidance to the stakeholders involved in or affected by the changes. The number of system software changes is a measure of how frequently and extensively the system software is modified or updated. System software changes are a type of change that affects the operating system, middleware, or utilities that support an information system.
While these three indicators are relevant and useful for measuring certain aspects of change management, they do not directly measure the outcomes or impacts of the changes on the organization. They are more related to the inputs or activities of change management than to its outputs or results. Therefore, they are not as appropriate indicators of change management effectiveness as the number of incidents resulting from changes.
Metrics for Measuring Change Management - Prosci
How to Measure Change Management Effectiveness: Metrics, Tools & Processes
Metrics for Measuring Change Management 2023 - Zendesk

QUESTION 144
An organization has recently moved to an agile model for deploying custom code to its in-house accounting software system. When reviewing the procedures in place for production code deployment, which of the following is the MOST significant security concern to address?

A. Software vulnerability scanning is done on an ad hoc basis.
B. Change control does not include testing and approval from quality assurance (QA).

C. Production code deployment is not automated.
D. Current DevSecOps processes have not been independently verified.

Correct Answer: B
Section:
Explanation:
Change control is the process of managing and documenting changes to an information system or its components. Change control aims to ensure that changes are authorized, tested, approved, implemented, and reviewed in a controlled and consistent manner. Change control is an essential part of ensuring the security, reliability, and quality of an information system.
One of the key elements of change control is testing and approval from quality assurance (QA). QA is the function that verifies that the changes meet the requirements and specifications, comply with the standards and policies, and do not introduce any errors or vulnerabilities. QA testing and approval provide assurance that the changes are fit for purpose, function as expected, and do not compromise the security or performance of the system.
An organization that has recently moved to an agile model for deploying custom code to its in-house accounting software system should still follow change control procedures, including QA testing and approval. Agile development methods emphasize flexibility, speed, and collaboration, but they do not eliminate the need for quality and security checks. In fact, agile methods can facilitate change control by enabling frequent and iterative testing and feedback throughout the development cycle.
However, if change control does not include testing and approval from QA, this poses a significant security concern for the organization. Without QA testing and approval, the changes may not be properly validated, verified, or evaluated before being deployed to production. This could result in introducing bugs, defects, or vulnerabilities that could affect the functionality, availability, integrity, or confidentiality of the accounting software system. For example, a change could cause data corruption, performance degradation, unauthorized access, or data leakage. These risks could have serious consequences for the organization's financial operations, compliance obligations, reputation, or legal liabilities.
Therefore, change control that does not include testing and approval from QA is the most significant security concern to address when reviewing the procedures in place for production code deployment in an agile model.
Change Control - ISACA
Quality Assurance - ISACA
Agile Development - ISACA
10 Agile Software Development Security Concerns You Need to Know

QUESTION 145
Which of the following provides a new IS auditor with the MOST useful information to evaluate overall IT performance?

A. IT value analysis
B. Prior audit reports
C. IT balanced scorecard
D. Vulnerability assessment report

Correct Answer: C
Section:
Explanation:
An IT balanced scorecard (BSC) is a performance metric that is used to identify, improve, and control the various functions and outcomes of an IT department or organization. An IT BSC is based on the concept of the balanced scorecard, which was introduced by Robert Kaplan and David Norton in 1992 as a strategic management system that translates the vision and strategy of an organization into measurable objectives and actions. An IT BSC adapts the balanced scorecard framework to the specific needs and goals of the IT function, aligning it with the business strategy and value proposition.
An IT BSC typically consists of four perspectives that help managers plan, implement, and evaluate the IT performance: customer, internal process, learning and growth, and financial. Each perspective defines a set of objectives, measures, targets, and initiatives that reflect the IT contribution to the organization's success. For example, the customer perspective may measure the satisfaction and retention of internal and external customers who use IT services or products; the internal process perspective may measure the efficiency and effectiveness of IT processes such as development, delivery, support, or security; the learning and growth perspective may measure the skills, knowledge, innovation, and culture of the IT staff; and the financial perspective may measure the costs, benefits, and return on investment of IT projects or assets.
An IT BSC provides a new IS auditor with the most useful information to evaluate overall IT performance because it:
Provides a comprehensive and balanced view of the IT function from multiple angles and stakeholders
Links the IT objectives and activities to the business strategy and value creation
Enables a clear communication and alignment of expectations and priorities among IT managers, staff, customers, and other stakeholders
Facilitates a continuous monitoring and improvement of IT performance based on data-driven feedback and analysis
Supports a holistic and integrated approach to IT governance, risk management, and compliance
Therefore, an IT BSC is a valuable tool for a new IS auditor to assess how well the IT function is fulfilling its mission and delivering value to the organization.

The IT Balanced Scorecard (BSC) Explained - BMC Software
What Is a Balanced Scorecard (BSC), How Is it Used in Business?
Lost in the Woods: COBIT 2019 and the IT Balanced Scorecard - ISACA

QUESTION 146
What is the MOST effective way to detect installation of unauthorized software packages by employees?

A. Regular scanning of hard drives
B. Communicating the policy to employees
C. Logging of activity on the network
D. Maintaining current antivirus software

Correct Answer: A
Section:
Explanation:
Regular scanning of hard drives is the most effective way to detect installation of unauthorized software packages by employees because it can identify any software that is not approved by the organization and may pose a security risk or violate the software policy. Communicating the policy to employees is important, but it may not prevent or detect unauthorized software installation. Logging of activity on the network can monitor network traffic, but it may not capture all software installation events. Maintaining current antivirus software can protect the system from malicious software, but it may not detect all unauthorized software packages.Reference:
ISACA, CISA Review Manual, 27th Edition, 2020, p.2381
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

QUESTION 147
Which of the following is MOST effective for controlling visitor access to a data center?

A. Visitors are escorted by an authorized employee
B. Pre-approval of entry requests
C. Visitors sign in at the front desk upon arrival
D. Closed-circuit television (CCTV) is used to monitor the facilities

Correct Answer: A
Section:
Explanation:
The most effective way for controlling visitor access to a data center is to ensure that visitors are escorted by an authorized employee, as this prevents unauthorized or malicious actions by the visitors and provides accountability and supervision.Pre-approval of entry requests, visitors signing in at the front desk upon arrival, and closed-circuit television (CCTV) are also useful measures, but they are not as effective as escorting visitors, as they do not prevent or detect unauthorized or malicious actions by the visitors in real time.Reference:CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Physical Access Controls1

QUESTION 148
Which of the following BEST enables an organization to improve the visibility of end-user computing (EUC) applications that support regulatory reporting?

A. EUC inventory
B. EUC availability controls
C. EUC access control matrix
D. EUC tests of operational effectiveness

Correct Answer: A
Section:
Explanation:
The best way to improve the visibility of end-user computing (EUC) applications that support regulatory reporting is to maintain an EUC inventory, as this provides a comprehensive and up-to-date list of all EUC applications,

their owners, their locations, their purposes, and their dependencies. An EUC inventory can help identify and manage the risks associated with EUC applications, such as data quality, security, compliance, and continuity.EUC availability controls, EUC access control matrix, and EUC tests of operational effectiveness are important for ensuring the reliability and security of EUC applications, but they do not improve the visibility of EUC applications as much as an EUC inventory.Reference:CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.4: End-user Computing

QUESTION 149
Which of the following provides the MOST useful information regarding an organization's risk appetite and tolerance?

A. Gap analysis
B. Audit reports
C. Risk profile
D. Risk register

Correct Answer: C
Section:
Explanation:
The most useful information regarding an organization's risk appetite and tolerance is provided by its risk profile, as this is a document that summarizes the key risks that the organization faces, the potential impacts and likelihoods of those risks, and the acceptable levels of risk exposure for different objectives and activities. A gap analysis is a tool that compares the current state and the desired state of a process or a system, and identifies the gaps that need to be addressed. Audit reports are documents that present the findings, conclusions, and recommendations of an audit engagement.A risk register is a tool that records and tracks the identified risks, their causes, their consequences, and their mitigation actions.Reference:CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.1: IT Governance

QUESTION 150
An organization has recently become aware of a pervasive chip-level security vulnerability that affects all of its processors. Which of the following is the BEST way to prevent this vulnerability from being exploited?

A. Implement security awareness training.
B. Install vendor patches
C. Review hardware vendor contracts.
D. Review security log incidents.

Correct Answer: B
Section:
Explanation:
The best way to prevent a chip-level security vulnerability from being exploited is to install vendor patches. A chip-level security vulnerability is a flaw in the design or implementation of a processor that allows an attacker to bypass the normal security mechanisms and access privileged information or execute malicious code. A vendor patch is a software update provided by the manufacturer of the processor that fixes or mitigates the vulnerability. Installing vendor patches can help to protect the system from known exploits and reduce the risk of data leakage or compromise.
Security awareness training, reviewing hardware vendor contracts, and reviewing security log incidents are not as effective as installing vendor patches for preventing a chip-level security vulnerability from being exploited. Security awareness training is an educational program that teaches users about the importance of security and how to avoid common threats. Reviewing hardware vendor contracts is a legal process that evaluates the terms and conditions of the agreement between the organization and the processor supplier. Reviewing security log incidents is an analytical process that examines the records of security events and activities on the system. These methods may be useful for other security purposes, but they do not directly address the root cause of the chip-level vulnerability or prevent its exploitation.Reference:Protecting your device against chip-related security vulnerabilities,New 'Downfall' Flaw Exposes Valuable Data in Generations of Intel Chips

QUESTION 151
Which of the following should be the GREATEST concern to an IS auditor reviewing an organization's method to transport sensitive data between offices?

A. The method relies exclusively on the use of public key infrastructure (PKI).
B. The method relies exclusively on the use of digital signatures.
C. The method relies exclusively on the use of asymmetric encryption algorithms.
D. The method relies exclusively on the use of 128-bit encryption.

Correct Answer: C
Section:
Explanation:
The greatest concern to an IS auditor reviewing an organization's method to transport sensitive data between offices is that the method relies exclusively on the use of asymmetric encryption algorithms. Asymmetric encryption algorithms, also known as public key encryption, use two different keys for encryption and decryption: a public key that is shared with anyone who wants to communicate with the sender, and a private key that is kept secret by the sender. Asymmetric encryption algorithms are more secure than symmetric encryption algorithms, which use the same key for both encryption and decryption, but they are also slower and more computationally intensive. Therefore, relying exclusively on asymmetric encryption algorithms may not be efficient or practical for transporting large amounts of sensitive data between offices. A better method would be to use a combination of symmetric and asymmetric encryption algorithms, such as using asymmetric encryption to exchange a symmetric key and then using symmetric encryption to encrypt and decrypt the data.
The other options are not as concerning as option C. The method relying exclusively on the use of public key infrastructure (PKI) is not a concern, because PKI is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates that are based on asymmetric encryption algorithms. PKI enables secure and authenticated communication between parties who do not have a prior trust relationship. The method relying exclusively on the use of digital signatures is not a concern, because digital signatures are a way of verifying the authenticity and integrity of a message or document by using asymmetric encryption algorithms. Digital signatures ensure that the sender cannot deny sending the message or document, and that the receiver can detect any tampering or alteration of the message or document. The method relying exclusively on the use of 128-bit encryption is not a concern, because 128-bit encryption is a level of encryption that uses a 128-bit key to encrypt and decrypt data. 128-bit encryption is considered to be strong enough to resist brute-force attacks by modern computers.Reference:Asymmetric vs Symmetric Encryption: What are differences?,Public Key Infrastructure (PKI),Digital Signature,What is 128-bit Encryption?

QUESTION 152
Which of the following is the BEST point in time to conduct a post-implementation review?

A. After a full processing cycle
B. Immediately after deployment
C. After the warranty period
D. Prior to the annual performance review

Correct Answer: A
Section:
Explanation:
The best point in time to conduct a post-implementation review is after a full processing cycle. A post-implementation review is a process to evaluate whether the objectives of the project were met, how effective the project was managed, what benefits were realized, and what lessons were learned. A post-implementation review should be conducted after a full processing cycle, which is the period of time required for a system or process to complete all its functions and produce its outputs. This allows for a more accurate and comprehensive assessment of the project's performance, outcomes, impacts, and issues.
The other options are not as good as option A. Conducting a post-implementation review immediately after deployment is too soon, because it does not allow enough time for the project's product or service to operate in the real world and generate measurable results. Conducting a post-implementation review after the warranty period is too late, because it may miss some important feedback or opportunities for improvement that could have been addressed earlier. Conducting a post-implementation review prior to the annual performance review is irrelevant, because it does not align with the project's life cycle or objectives.Reference:What is Post-Implementation Review in Project Management?,What Is the Post-Implementation Review (PIR) Process?,Post-implementation review in project management?

QUESTION 153
During a project audit, an IS auditor notes that project reporting does not accurately reflect current progress. Which of the following is the GREATEST resulting impact?

A. The project manager will have to be replaced.
B. The project reporting to the board of directors will be incomplete.
C. The project steering committee cannot provide effective governance.
D. The project will not withstand a quality assurance (QA) review.

Correct Answer: C
Section:
Explanation:
The greatest resulting impact of project reporting not accurately reflecting current progress is that the project steering committee cannot provide effective governance. The project steering committee is a group of senior executives or stakeholders who oversee the project and provide strategic direction, guidance, and support. The project steering committee relies on accurate and timely project reporting to monitor the project's status, performance, risks, issues, and changes. If the project reporting is inaccurate, the project steering committee cannot make informed decisions, resolve problems, allocate resources, or ensure alignment with the organizational goals and objectives.

The other options are not as impactful as option C. The project manager will have to be replaced is a possible consequence, but not the greatest impact, of inaccurate project reporting. The project manager is responsible for planning, executing, monitoring, controlling, and closing the project. The project manager may face disciplinary actions or termination if they fail to provide accurate and honest project reporting. However, this does not necessarily affect the overall governance of the project. The project reporting to the board of directors will be incomplete is a potential risk, but not the greatest impact, of inaccurate project reporting. The board of directors is the highest governing body of an organization that sets the vision, mission, values, and policies. The board of directors may receive periodic or ad hoc project reporting to ensure that the project is aligned with the organizational strategy and delivers value. If the project reporting is inaccurate, the board of directors may lose confidence in the project or intervene in its management. However, this does not directly affect the day-to-day governance of the project. The project will not withstand a quality assurance (QA) review is a possible outcome, but not the greatest impact, of inaccurate project reporting. A quality assurance review is a process to evaluate the quality of the project's processes and deliverables against predefined standards and criteria. A quality assurance review may reveal discrepancies or errors in the project reporting that may affect the credibility and reliability of the project. However, this does not necessarily affect the governance of the project.Reference:Project Steering Committee - Roles & Responsibilities,Project Reporting Best Practices,Quality Assurance in Project Management

QUESTION 154
What should an IS auditor evaluate FIRST when reviewing an organization's response to new privacy legislation?

A. Implementation plan for restricting the collection of personal information
B. Privacy legislation in other countries that may contain similar requirements
C. Operational plan for achieving compliance with the legislation
D. Analysis of systems that contain privacy components

Correct Answer: D
Section:
Explanation:
The first thing that an IS auditor should evaluate when reviewing an organization's response to new privacy legislation is the analysis of systems that contain privacy components. Privacy components are elements of a system that collect, process, store, or transmit personal information that is subject to privacy legislation. An analysis of systems that contain privacy components should identify what types of personal information are involved, where they are located, how they are used, who has access to them, and what risks or threats they face. An analysis of systems that contain privacy components is essential for determining the scope and impact of the new privacy legislation on the organization's systems and processes.
The other options are not as important as option D. An implementation plan for restricting the collection of personal information is a possible action, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An implementation plan for restricting the collection of personal information is a document that outlines how an organization will comply with the principle of data minimization, which states that personal information should be collected only for specific and legitimate purposes and only to the extent necessary for those purposes. An implementation plan for restricting the collection of personal information should be based on an analysis of systems that contain privacy components. Privacy legislation in other countries that may contain similar requirements is a possible source of reference, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. Privacy legislation in other countries that may contain similar requirements is a set of laws or regulations that governs the protection of personal information in other jurisdictions that may have comparable or compatible standards or expectations as the new privacy legislation. Privacy legislation in other countries that may contain similar requirements may provide guidance or best practices for complying with the new privacy legislation. However, privacy legislation in other countries that may contain similar requirements should not be used as a substitute for an analysis of systems that contain privacy components. An operational plan for achieving compliance with the legislation is a possible deliverable, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An operational plan for achieving compliance with the legislation is a document that describes how an organization will implement and maintain the necessary policies, procedures, controls, and measures to comply with the new privacy legislation. An operational plan for achieving compliance with the legislation should be derived from an analysis of systems that contain privacy components.Reference: Privacy law - Wikipedia,Data Protection and Privacy Legislation Worldwide | UNCTAD,Data minimization - Wikipedia

QUESTION 155
Which of the following is MOST important to include in security awareness training?

A. How to respond to various types of suspicious activity
B. The importance of complex passwords
C. Descriptions of the organization's security infrastructure
D. Contact information for the organization's security team

Correct Answer: A
Section:
Explanation:
The most important thing to include in security awareness training is how to respond to various types of suspicious activity. Security awareness training is a program that educates employees about the importance of security

and how to avoid common threats and risks. One of the main objectives of security awareness training is to enable employees to recognize and report any signs of malicious or unauthorized activity, such as phishing emails, malware infections, data breaches, or social engineering attempts. By teaching employees how to respond to various types of suspicious activity, security awareness training can help to prevent or mitigate the impact of security incidents, protect the organization's assets and reputation, and comply with legal and regulatory requirements.
The other options are not as important as option A. The importance of complex passwords is a useful topic, but not the most important thing to include in security awareness training. Complex passwords are passwords that are hard to guess or crack by using a combination of letters, numbers, symbols, and cases. Complex passwords can help to protect user accounts and data from unauthorized access, but they are not sufficient to prevent all types of security incidents. Moreover, complex passwords may be difficult to remember or manage by users, and may require additional measures such as password managers or multi-factor authentication. Descriptions of the organization's security infrastructure is a technical topic, but not the most important thing to include in security awareness training. Security infrastructure is the set of hardware, software, policies, and procedures that provide the foundation for the organization's security posture and capabilities. Security infrastructure may include firewalls, antivirus software, encryption tools, access control systems, backup systems, etc. Descriptions of the organization's security infrastructure may be relevant for some employees who are involved in security operations or administration, but they may not be necessary or understandable for all employees who need security awareness training. Contact information for the organization's security team is a practical detail, but not the most important thing to include in security awareness training. Security team is the group of people who are responsible for planning, implementing, monitoring, and improving the organization's security strategy and activities. Contact information for the organization's security team may be useful for employees who need to report or escalate a security issue or request a security service or support. However, contact information for the organization's security team is not enough to ensure that employees know how to respond to various types of suspicious activity.Reference:Security Awareness Training | SANS Security Awareness,Security Awareness Training | KnowBe4,Security Awareness Training Course (ISC) | Coursera

QUESTION 156
A core system fails a week after a scheduled update, causing an outage that impacts service. Which of the following is MOST important for incident management to focus on when addressing the issue?

A. Analyzing the root cause of the outage to ensure the incident will not reoccur
B. Restoring the system to operational state as quickly as possible
C. Ensuring all resolution steps are fully documented prior to returning the system to service
D. Rolling back the unsuccessful change to the previous state

Correct Answer: B
Section:
Explanation:
The most important thing for incident management to focus on when addressing an issue that causes an outage is restoring the system to operational state as quickly as possible. Incident management is the process of detecting, investigating, and resolving incidents that disrupt or degrade a service or system. An incident is an unplanned event that affects the normal functioning or quality of a service or system. An outage is a type of incident that causes a complete loss of service or system availability. The main goal of incident management is to restore the service or system to its operational state as quickly as possible, minimizing the impact on users and business operations.
*The other options are not as important as option B. Analyzing the root cause of the outage to ensure the incident will not re-occur is a valuable activity, but not the most important thing for incident management to focus on when addressing an issue that causes an outage. Root cause analysis is a process of identifying and eliminating the underlying factors that caused an incident or problem. Root cause analysis can help to prevent or reduce the likelihood of similar incidents or problems in the future. However, root cause analysis is usually performed after the incident has been resolved and the service or system has been restored. Ensuring all resolution steps are fully documented prior to returning the system to service is a good practice, but not the most important thing for incident management to focus on when addressing an issue that causes an outage. Documentation is a process of recording and maintaining information about an incident and its resolution steps. Documentation can help to improve communication, accountability, learning, and improvement within incident management. However, documentation should not delay or interfere with the restoration of the service or system. Rolling back the unsuccessful change to the previous state is a possible solution, but not the most important thing for incident management to focus on when addressing an issue that causes an outage. Rolling back is a process of reverting a change that has been applied to a service or system that caused an incident or problem. Rolling back can help to restore the service or system to its previous state before the change was made.

QUESTION 157
Which of the following is MOST helpful for an IS auditor to review when evaluating an organizations business process that are supported by applications and IT systems?

A. Configuration management database (CMDB)
B. Enterprise architecture (EA)
C. IT portfolio management
D. IT service management

Correct Answer: B
Section:
Explanation:

The most helpful thing for an IS auditor to review when evaluating an organization's business processes that are supported by applications and IT systems is the enterprise architecture (EA). EA is the practice of designing a business with a holistic view, considering all of its parts and how they interact. EA defines the overall goals, the strategies that support those goals, and the tactics that are needed to execute those strategies. EA also outlines the ways various components of IT projects interact with one another and with the business processes. By reviewing the EA, an IS auditor can gain a comprehensive understanding of how the organization aligns its IT efforts with its overall mission, business strategy, and priorities. An IS auditor can also assess the effectiveness, efficiency, agility, and continuity of complex business operations.
The other options are not as helpful as option B. A configuration management database (CMDB) is a database that stores and manages information about the components that make up an IT system. A CMDB tracks individual configuration items (CIs), such as hardware, software, or data assets, and their attributes, dependencies, and changes over time. A CMDB can help an IS auditor to monitor the performance, availability, and configuration of IT assets, but it does not provide a holistic view of how they support the business processes. IT portfolio management is the practice of managing IT investments, projects, and activities as a portfolio. IT portfolio management aims to optimize the value, risk, and cost of IT initiatives and align them with the business objectives. IT portfolio management can help an IS auditor to evaluate the return on IT investments and the alignment of IT projects with the business strategy, but it does not provide a detailed view of how they support the business processes. IT service management (ITSM) is the practice of planning, implementing, managing, and optimizing IT services to meet the needs of end users and customers. ITSM focuses on delivering IT as a service using standardized processes and best practices. ITSM can help an IS auditor to review the quality, efficiency, and effectiveness of IT service delivery and support, but it does not provide a comprehensive view of how they support the business processes.Reference:What is enterprise architecture (EA)? - RingCentral,What is a configuration management database (CMDB)? - Red Hat,IT Portfolio Management Strategies | Smartsheet,What is IT service management (ITSM)? | IBM

QUESTION 158
Which of the following would be of GREATEST concern to an IS auditor reviewing an IT strategy document?

A. Target architecture is defined at a technical level.
B. The previous year's IT strategic goals were not achieved.
C. Strategic IT goals are derived solely from the latest market trends.
D. Financial estimates of new initiatives are disclosed within the document.

Correct Answer: C
Section:
Explanation:
The most concerning thing for an IS auditor reviewing an IT strategy document is that the strategic IT goals are derived solely from the latest market trends. An IT strategy document is a blueprint that defines how an organization will use technology to achieve its goals. It should be based on a thorough analysis of the organization's internal and external factors, such as its vision, mission, values, objectives, strengths, weaknesses, opportunities, threats, customers, competitors, regulations, and industry standards. An IT strategy document should also align with the organization's business strategy and reflect its unique needs and capabilities. If an IT strategy document is derived solely from the latest market trends, it may not be relevant or appropriate for the organization's specific situation. It may also lack coherence, consistency, feasibility, or sustainability.
The other options are not as concerning as option C. Target architecture is defined at a technical level is not a concern for an IS auditor reviewing an IT strategy document. Target architecture is the desired state of an organization's IT systems in terms of their structure, functionality, performance, security, interoperability, and integration. Defining target architecture at a technical level can help an IS auditor to understand how the organization plans to achieve its strategic IT goals and what technical requirements and standards it needs to follow. The previous year's IT strategic goals were not achieved is not a concern for an IS auditor reviewing an IT strategy document. The previous year's IT strategic goals are the outcomes that the organization intended to accomplish with its IT initiatives in the past year. Not achieving these goals may indicate some challenges or gaps in the organization's IT performance or execution. However, this does not necessarily affect the quality or validity of the current IT strategy document. An IS auditor should focus on evaluating whether the current IT strategy document is realistic, measurable, achievable, relevant, and time-bound. Financial estimates of new initiatives are disclosed within the document is not a concern for an IS auditor reviewing an IT strategy document. Financial estimates are projections of the costs and benefits of new initiatives that are part of the IT strategy document. Disclosing financial estimates within the document can help an IS auditor to assess whether the new initiatives are aligned with the organization's budget and resources and whether they provide value for money.Reference:IT Strategy Template for a Successful Strategic Plan | Gartner,Definitive Guide to Developing an IT Strategy and Roadmap - CioPages,An Example of a Well-Developed IT Strategy Plan - Resolute

QUESTION 159
An organization has shifted from a bottom-up approach to a top-down approach in the development of IT policies. This should result in:

A. greater consistency across the organization.
B. a synthesis of existing operational policies.
C. a more comprehensive risk assessment plan.
D. greater adherence to best practices.

Correct Answer: A
Section:
Explanation:

A top-down approach in the development of IT policies means that the policies are derived from the strategic objectives and goals of the organization, and are aligned with the business needs and expectations. This should result in greater consistency across the organization, as the policies will be coherent, integrated and applicable to all levels and functions of the organization. A bottom-up approach, on the other hand, means that the policies are developed by individual units or departments based on their operational needs and preferences, which may lead to inconsistency, duplication or conflict among different policies.Reference:ISACA Frameworks: Blueprints for Success,IT Governance and Process Maturity

QUESTION 160
An organization considering the outsourcing of a business application should FIRST:

A. define service level requirements.
B. perform a vulnerability assessment.
C. conduct a cost-benefit analysis.
D. issue a request for proposal (RFP).

Correct Answer: C
Section:
Explanation:
An organization considering the outsourcing of a business application should first conduct a cost-benefit analysis to evaluate the feasibility, viability and desirability of the outsourcing decision. A cost-benefit analysis should compare the costs and benefits of outsourcing versus keeping the application in-house, taking into account factors such as financial, operational, strategic, legal, regulatory, security and quality aspects. A cost-benefit analysis should also identify the risks and opportunities associated with outsourcing, and provide a basis for defining the service level requirements, performing a vulnerability assessment, and issuing a request for proposal (RFP) in the subsequent stages of the outsourcing process.Reference:Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA,CISA Certification | Certified Information Systems Auditor | ISACA

QUESTION 161
Which of the following is an example of a preventive control for physical access?

A. Keeping log entries for all visitors to the building
B. Implementing a fingerprint-based access control system for the building
C. Installing closed-circuit television (CCTV) cameras for all ingress and egress points
D. Implementing a centralized logging server to record instances of staff logging into workstations

Correct Answer: B
Section:
Explanation:
A preventive control is a control that aims to deter or prevent undesirable events from occurring. A fingerprint-based access control system for the building is an example of a preventive control for physical access, as it restricts unauthorized persons from entering the premises. Keeping log entries for all visitors to the building, installing CCTV cameras for all ingress and egress points, and implementing a centralized logging server to record instances of staff logging into workstations are examples of detective controls, which are controls that aim to discover or detect undesirable events that have already occurred.

QUESTION 162
The BEST way to evaluate the effectiveness of a newly developed application is to:

A. perform a post-implementation review-
B. analyze load testing results.
C. perform a secure code review.
D. review acceptance testing results.

Correct Answer: D
Section:
Explanation:
The best way to evaluate the effectiveness of a newly developed application is to review acceptance testing results. Acceptance testing is a process of verifying that the application meets the specified requirements and

expectations of the users and stakeholders. Acceptance testing results can provide evidence of the functionality, usability, reliability, performance, security and quality of the application. Performing a post-implementation review, analyzing load testing results, and performing a secure code review are also important activities for evaluating an application, but they are not as comprehensive or conclusive as acceptance testing results.

QUESTION 163
Which of the following is the PRIMARY objective of implementing privacy-related controls within an organization?

A. To prevent confidential data loss
B. To comply with legal and regulatory requirements
C. To identify data at rest and data in transit for encryption
D. To provide options to individuals regarding use of their data

Correct Answer: B
Section:
Explanation:
The primary objective of implementing privacy-related controls within an organization is to comply with legal and regulatory requirements that protect the rights and interests of individuals whose personal data are collected, processed, stored, shared or disposed by the organization. Privacy-related controls are based on principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. These principles aim to ensure that personal data are processed in a manner that respects the privacy of individuals and complies with the applicable laws and regulations in different jurisdictions. Preventing confidential data loss, identifying data at rest and data in transit for encryption, and providing options to individuals regarding use of their data are examples of specific privacy-related controls that support the primary objective of compliance.Reference:Privacy Regulatory Lookup Tool,CDPSE Official Review Manual, 2nd Edition

QUESTION 164
Which type of attack targets security vulnerabilities in web applications to gain access to data sets?

A. Denial of service (DOS)
B. SQL injection
C. Phishing attacks
D. Rootkits

Correct Answer: B
Section:
Explanation:
A SQL injection attack is a type of attack that targets security vulnerabilities in web applications to gain access to data sets. A SQL injection attack exploits a flaw in the web application code that allows an attacker to inject malicious SQL statements into the input fields or parameters of the web application. These SQL statements can then execute on the underlying database server and manipulate or retrieve sensitive data from the database. A SQL injection attack can result in data theft, data corruption, unauthorized access, denial of service or even complete takeover of the database server. A denial of service (DOS) attack is a type of attack that aims to disrupt the availability or functionality of a web application or a network service by overwhelming it with excessive requests or traffic. A phishing attack is a type of attack that uses deceptive emails or websites to trick users into revealing their personal or financial information or credentials. A rootkit is a type of malware that hides itself from detection and grants unauthorized access or control over a compromised system.Reference:IS Audit and Assurance Tools and Techniques,CISA Certification | Certified Information Systems Auditor | ISACA

QUESTION 165
An organization that operates an e-commerce website wants to provide continuous service to its customers and is planning to invest in a hot site due to service criticality. Which of the following is the MOST important consideration when making this decision?

A. Maximum tolerable downtime (MTD)
B. Recovery time objective (RTO)
C. Recovery point objective (RPO)
D. Mean time to repair (MTTR)

Correct Answer: B

Section:
Explanation:
The recovery time objective (RTO) is the most important consideration when making a decision to invest in a hot site due to service criticality. The RTO is the maximum acceptable time that an IT service or process can be unavailable or disrupted before it causes significant damage to the business operations and objectives. A hot site is a fully equipped and operational backup facility that can be activated immediately in the event of a disaster or disruption. A hot site can help an organization achieve a very low RTO, as it can resume the service with minimal or no downtime. The maximum tolerable downtime (MTD) is the maximum acceptable time that an IT service or process can be unavailable or disrupted before it causes intolerable damage to the business operations and objectives. The MTD is usually longer than the RTO, as it represents the worst-case scenario. The recovery point objective (RPO) is the maximum acceptable amount of data loss that an IT service or process can tolerate in the event of a disaster or disruption. The RPO is measured in terms of time, such as hours or minutes, and indicates how frequently the data should be backed up or replicated. The mean time to repair (MTTR) is the average time that it takes to restore an IT service or process after a failure or disruption. The MTTR is a measure of the efficiency and effectiveness of the recovery process, but it does not reflect the service criticality or the business impact.Reference:IS Audit and Assurance Tools and Techniques,CISA Certification | Certified Information Systems Auditor | ISACA

QUESTION 166
Which of the following is an IS auditor's BEST recommendation for mitigating risk associated with inadvertent disclosure of sensitive information by employees?

A. Intrusion prevention system (IPS) and firewalls
B. Data loss prevention (DLP) technologies
C. Cryptographic protection
D. Email phishing simulation exercises

Correct Answer: B
Section:
Explanation:
DLP technologies are designed to prevent the unauthorized transmission or leakage of sensitive data, such as PII, intellectual property, or financial information, by employees or other insiders. DLP technologies can monitor, detect, and block data in motion, data at rest, and data in use across various channels, such as email, web, cloud, or removable devices. DLP technologies can also help enforce data security policies and compliance requirements.
Reference
ISACA CISA Review Manual, 27th Edition, page 253
The role of disclosures in risk assessment and mitigation
Mitigate Risk Strategy for Information Management

QUESTION 167
Which of the following will provide the GREATEST assurance to IT management that a quality management system (QMS) is effective?

A. A high percentage of stakeholders satisfied with the quality of IT
B. Ahigh percentage of incidents being quickly resolved
C. Ahigh percentage of IT processes reviewed by quality assurance (QA)
D. Ahigh percentage of IT employees attending quality training

Correct Answer: A
Section:
Explanation:
Stakeholder satisfaction is a key indicator of the effectiveness of a QMS, as it reflects the extent to which the QMS meets the expectations and priorities of the customers and other interested parties. A high percentage of stakeholder satisfaction implies that the QMS is delivering consistent and reliable products or services that meet the quality standards and requirements.
Reference
ISACA CISA Review Manual, 27th Edition, page 253
The Four Main Components of A Quality Management System
The Road to Developing an Effective Quality Management System (QMS)

QUESTION 168

Which of the following is the GREATEST risk associated with hypervisors in virtual environments?

A. Availability issues
B. Virtual sprawl
C. Single point of failure
D. Lack of patches

Correct Answer: C
Section:
Explanation:
A single point of failure is a component or system that, if it fails, will cause the entire system to stop functioning. In virtual environments, the hypervisor is the software layer that enables multiple virtual machines to run on a single physical host. If the hypervisor is compromised, corrupted, or unavailable, all the virtual machines running on that host will be affected. This can result in data loss, downtime, or security breaches.
Reference
ISACA CISA Review Manual, 27th Edition, page 254
Virtualization: What are the security risks?
What Is a Hypervisor? (Definition, Types, Risks)

QUESTION 169
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's incident response management program?

A. All incidents have a severity level assigned.
B. All identified incidents are escalated to the CEO and the CISO.
C. Incident response is within defined service level agreements (SLAs).
D. The alerting tools and incident response team can detect incidents.

Correct Answer: D
Section:
Explanation:
The most important aspect of an incident response management program is the ability to detect incidents in a timely and accurate manner. Without effective detection, the organization cannot respond to incidents, mitigate their impact, or prevent their recurrence. The alerting tools and incident response team are responsible for monitoring the IT environment, identifying anomalies or threats, and notifying the appropriate stakeholders.
Reference
ISACA CISA Review Manual, 27th Edition, page 255
What is an incident response plan? And why do you need one?
ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB

QUESTION 170
Which of the following is MOST appropriate to review when determining if the work completed on an IT project is in alignment with budgeted costs?

A. Return on investment (ROI) analysis
B. Earned value analysis (EVA)
C. Financial value analysis
D. Business impact analysis (BIA)

Correct Answer: B
Section:
Explanation:
EVA is a project management technique that measures the performance of a project by comparing the actual work completed, the actual costs incurred, and the planned costs for the work scheduled. EVA can help determine if the project is on track, ahead of schedule, or behind schedule, and if the project is under budget, over budget, or on budget. EVA can also help forecast the final cost and schedule of the project based on the current

performance.
Reference
ISACA CISA Review Manual, 27th Edition, page 255
18. Project Completion -- Project Management -- 2nd Edition
How to Measure Project Success | Smartsheet

QUESTION 171
The PRIMARY reason to perform internal quality assurance (QA) for an internal audit function is to ensure:

A. audit resources are used most effectively.
B. internal audit activity conforms with audit standards and methodology.
C. the audit function is adequately governed and meets performance metrics.
D. inherent risk in audits is minimized.

Correct Answer: B
Section:
Explanation:
The primary reason to perform internal QA for an internal audit function is to ensure that the internal audit activity adheres to the Definition of Internal Auditing and the International Standards for the Professional Practice of Internal Auditing (Standards) issued by the Institute of Internal Auditors (IIA), as well as the internal audit methodology and policies of the organization. A QA program enables an evaluation of the internal audit activity's performance, efficiency, effectiveness, and value, and identifies opportunities for improvement. A QA program also helps to enhance the credibility and reputation of the internal audit function among the stakeholders.
Reference
Quality Assurance - The Institute of Internal Auditors or The IIA
Benefits of a quality assurance review for internal audit
Optimize your internal audit function with a quality assurance review ...

QUESTION 172
Which of the following presents the GREATEST risk to an organization's ability to manage quality control (QC) processes?

A. Lack of segregation of duties
B. Lack of a dedicated QC function
C. Lack of policies and procedures
D. Lack of formal training and attestation

Correct Answer: C
Section:
Explanation:
The greatest risk to an organization's ability to manage QC processes is the lack of policies and procedures that define the QC objectives, standards, methods, roles, and responsibilities. Without policies and procedures, the QC processes may be inconsistent, ineffective, inefficient, or noncompliant with the relevant regulations and best practices. Policies and procedures provide the foundation and guidance for the QC processes and help to ensure their quality, reliability, and accountability.
Reference
ISACA CISA Review Manual, 27th Edition, page 253
Quality Control - an overview | ScienceDirect Topics
Quality Control: Meaning, Importance, Definition and Objectives

QUESTION 173
A configuration management audit identified that predefined automated procedures are used when deploying and configuring application infrastructure in a cloud-based environment. Which of the following is MOST important for the IS auditor to review?

A. Storage location of configuration management documentation
B. Processes for making changes to cloud environment specifications
C. Contracts of vendors responsible for maintaining provisioning tools
D. Number of administrators with access to cloud management consoles

Correct Answer: B
Section:
Explanation:
The IS auditor should review the processes for making changes to cloud environment specifications, as these are the inputs for the predefined automated procedures that deploy and configure the application infrastructure. The IS auditor should verify that the changes are authorized, documented, tested, and approved before they are applied to the cloud environment. The IS auditor should also check that the changes are aligned with the business requirements and do not introduce any security or performance issues.
Reference
ISACA CISA Review Manual, 27th Edition, page 254
Configuration Management in Cloud Computing - ScienceDirect
Cloud Configuration Management - BMC Software

QUESTION 174
Which of the following is the MOST effective way to detect as many abnormalities as possible during an IS audit?

A. Conduct a walk-through of the process.
B. Perform substantive testing on sampled records.
C. Perform judgmental sampling of key processes.
D. Use a data analytics tool to identify trends.

Correct Answer: D
Section:
Explanation:
A data analytics tool is the most effective way to detect as many abnormalities as possible during an IS audit, as it can process large volumes of data, perform complex calculations, and generate visualizations that reveal patterns, outliers, anomalies, or deviations from expected results. A data analytics tool can also help the auditor to test the entire population of data, rather than a sample, and to perform continuous auditing and monitoring.
Reference
ISACA CISA Review Manual, 27th Edition, page 256
What is Problem Solving? Steps, Process & Techniques | ASQ
Data Analytics for Auditors - IIA

QUESTION 175
Which of the following is a PRIMARY benefit of using risk assessments to determine areas to be included in an audit plan?

A. Timely audit execution
B. Effective allocation of audit resources
C. Reduced travel and expense costs
D. Effective risk mitigation

Correct Answer: B
Section:
Explanation:
Using risk assessments to determine areas to be included in an audit plan is a primary benefit because it helps to prioritize the audit activities based on the level of risk and the potential impact of the audit findings. This way, the audit resources, such as time, staff, and budget, can be allocated more efficiently and effectively to the areas that need the most attention and provide the most value.
Reference

ISACA CISA Review Manual, 27th Edition, page 256
What is the Purpose of a Risk Assessment?
Mastering the Process of Risk Assessment

QUESTION 176
An IS auditor is conducting an IT governance audit and notices many initiatives are managed informally by isolated project managers. Which of the following recommendations would have the GREATEST impact on improving the maturity of the IT team?

A. Schedule a follow-up audit in the next year to confirm whether IT processes have matured.
B. Create an interdisciplinary IT steering committee to oversee IT prioritization and spending.
C. Document and track all IT decisions in a project management tool.
D. Discontinue all current IT projects until formal approval is obtained and documented.

Correct Answer: B
Section:
Explanation:
An IT steering committee is a group of senior executives and stakeholders who provide strategic direction, guidance, and oversight for the IT function of an organization. An IT steering committee can help to improve the maturity of the IT team by ensuring that the IT initiatives are aligned with the business goals and objectives, that the IT resources are allocated and utilized effectively and efficiently, and that the IT performance and value are measured and communicated. An IT steering committee can also help to resolve conflicts, prioritize demands, and foster collaboration among the IT project managers and other business units.
Reference
ISACA CISA Review Manual, 27th Edition, page 254
Auditing IT Governance
The Impact of Poor IT Audit Planning and Mitigating Audit Risk
IS Audit Basics: The Components of the IT Audit Report

QUESTION 177
Which of the following should be the GREATEST concern for an IS auditor assessing an organization's disaster recovery plan (DRP)?

A. The DRP was developed by the IT department.
B. The DRP has not been tested during the past three years.
C. The DRP has not been updated for two years.
D. The DRP does not include the recovery the time objective (RTO) for a key system.

Correct Answer: B
Section:
Explanation:
The DRP is a set of procedures and resources that enable an organization to restore its critical IT functions and operations in the event of a disaster or disruption. The DRP should be tested regularly to ensure its effectiveness, validity, and readiness. Testing the DRP can help to identify and resolve any gaps, issues, or weaknesses in the plan, as well as to evaluate the performance and capability of the recovery team and resources. If the DRP has not been tested during the past three years, it may not reflect the current IT environment, business requirements, or recovery objectives, and it may fail to meet the expectations and needs of the stakeholders.
Reference
ISACA CISA Review Manual, 27th Edition, page 255
Disaster Recovery Plan Testing: The Ultimate Checklist
What is a Disaster Recovery Plan (DRP) and How Do You Write One?

QUESTION 178
A programmer has made unauthorized changes to key fields in a payroll system report. Which of the following control weaknesses would have contributed MOST to this problem?

A. The programmer did not involve the user in testing.

B. The user requirements were not documented.
C. Payroll files were not under the control of a librarian.
D. The programmer has access to the production programs.

Correct Answer: D
Section:
Explanation:
The programmer having access to the production programs is the most likely control weakness that would have contributed to the unauthorized changes to the payroll system report. This is because the programmer could modify the production code without proper authorization, documentation, or testing, and bypass the change management process. This could result in errors, fraud, or data integrity issues in the payroll system. The programmer should only have access to the development or test environment, and the production programs should be under the control of a librarian or a change manager.
Reference
ISACA CISA Review Manual, 27th Edition, page 254
4 Types of Internal Control Weaknesses
ACCT 4631 - Internal Auditing: CIA Quiz Topic 6 Flashcards

QUESTION 179
Which of the following is MOST important when defining the IS audit scope?

A. Minimizing the time and cost to the organization of IS audit procedures
B. Involving business in the formulation of the scope statement
C. Aligning the IS audit procedures with IT management priorities
D. Understanding the relationship between IT and business risks

Correct Answer: D
Section:
Explanation:
The most important factor when defining the IS audit scope is to understand the relationship between IT and business risks, as this helps to identify the areas that have the most potential impact on the organization's objectives, performance, and value. By understanding the IT and business risks, the IS auditor can focus the audit scope on the key processes, systems, controls, and issues that need to be assessed and addressed.
Reference
ISACA CISA Review Manual, 27th Edition, page 256
Ten Factors to Consider when Setting the Scope of an Internal Audit
What Is an Audit Scope? | Auditing Basics | KirkpatrickPrice

QUESTION 180
An IS auditor is assessing the adequacy of management's remediation action plan. Which of the following should be the MOST important consideration?

A. Plan approval by the audit committee
B. Impacts on future audit work
C. Criticality of audit findings
D. Potential cost savings

Correct Answer: C
Section:
Explanation:
The most important consideration when assessing the adequacy of management's remediation action plan is the criticality of the audit findings, as this reflects the level of risk and impact that the findings pose to the organization's objectives, performance, and value. The IS auditor should evaluate whether the remediation action plan addresses the root causes, mitigates the risks, and resolves the issues of the audit findings in a timely and effective manner. The IS auditor should also consider the feasibility, reasonableness, and measurability of the remediation actions.
Reference

ISACA CISA Review Manual, 27th Edition, page 256
How to Write an Audit Finding - Dallas Chapter of the IIA
How to Write an Audit Report: 14 Steps (with Pictures) - wikiHow

QUESTION 181
During a physical security audit, an IS auditor was provided a proximity badge that granted access to three specific floors in a corporate office building. Which of the following issues should be of MOST concern?

A. The proximity badge did not work for the first two days of audit fieldwork.
B. There was no requirement for an escort during fieldwork.
C. There was no follow-up for unsuccessful attempted access violations.
D. The proximity badge incorrectly granted access to restricted areas.

Correct Answer: D
Section:
Explanation:
The proximity badge incorrectly granting access to restricted areas is the most concerning issue, as it indicates a failure of the access control system to enforce the principle of least privilege and protect the sensitive or critical assets of the organization. The proximity badge should only grant access to the areas that are necessary for the IS auditor to perform the audit fieldwork, and not to any other areas that may contain confidential information, valuable equipment, or hazardous materials. The incorrect access could result in unauthorized disclosure, modification, or destruction of the assets, as well as potential safety or legal issues.
Reference
ISACA CISA Review Manual, 27th Edition, page 254
Office & Workplace Physical Security Assessment Checklist
Physical Security: Planning, Measures & Examples

QUESTION 182
Which of the following BEST ensures that effective change management is in place in an IS environment?

A. User authorization procedures for application access are well established.
B. User-prepared detailed test criteria for acceptance testing of the software.
C. Adequate testing was carried out by the development team.
D. Access to production source and object programs is well controlled.

Correct Answer: D
Section:
Explanation:
Access to production source and object programs is the best way to ensure that effective change management is in place in an IS environment, as it prevents unauthorized or accidental changes to the production code that could affect the functionality, performance, or security of the system. Access to production source and object programs should be restricted to authorized personnel only, and any changes should follow a formal change management process that includes documentation, approval, testing, and review.
Reference
ISACA CISA Review Manual, 27th Edition, page 254
Change Management Best Practices for the Engineering and ...
Change Management - an overview | ScienceDirect Topics

QUESTION 183
An IS auditor discovers from patch logs that some in-scope systems are not compliant with the regular patching schedule. What should the auditor do NEXT?

A. Interview IT management to clarify the current procedure.
B. Report this finding to senior management.
C. Review the organization's patch management policy.

D. Request a plan of action to be established as a follow-up item.

Correct Answer: C
Section:
Explanation:
The IS auditor should review the organization's patch management policy to determine the expected frequency and scope of patching, as well as the roles and responsibilities of the patch management team.This will help the auditor assess the severity and impact of the non-compliance, and identify the root cause and possible remediation actions12.
Reference
1: How to Create a Patch Management Policy: Complete Guide2: Free Patch Management Policy Template (+Examples)

QUESTION 184
Which of the following applications has the MOST inherent risk and should be prioritized during audit planning?

A. A decommissioned legacy application
B. An onsite application that is unsupported
C. An outsourced accounting application
D. An internally developed application

Correct Answer: C
Section:
Explanation:
An outsourced accounting application has the most inherent risk and should be prioritized during audit planning because it involves external parties, sensitive data, and complex transactions that are susceptible to material misstatement, error, or fraud12.An outsourced accounting application also requires more oversight and monitoring from the internal audit department to ensure compliance with the service level agreement and the organization's policies and standards3.
Reference
1: Inherent Risk: Definition, Examples, and 3 Types of Audit Risks2: 3 Types of Audit Risk - Inherent, Control and Detection - Accountinguide3: IS Audit Basics: The Core of IT Auditing

QUESTION 185
During an audit of payment services of a branch based in a foreign country, a large global bank's audit team identifies an opportunity to use data analytics techniques to identify abnormal payments. Which of the following is the team's MOST important course of action?

A. Consult the legal department to understand the procedure for requesting data from a different jurisdiction.
B. Conduct a walk through of the analytical strategy with stakeholders of the audited branch to obtain their buy-in.
C. Request the data from the branch as the team audit charter covers the country where it is based.
D. Agree on a data extraction and sharing strategy with the IT team of the audited branch.

Correct Answer: A
Section:
Explanation:
The audit team's most important course of action is to consult the legal department to understand the procedure for requesting data from a different jurisdiction, as this will ensure that the data analytics techniques are compliant with the applicable laws and regulations of both countries12.Requesting data from a foreign branch may involve legal risks such as data privacy, data sovereignty, and data protection34, and the audit team should seek legal guidance before proceeding with the data extraction and analysis.
Reference
1: Data Analytics and Auditing Standards2: Data Analytics and the Audit Process3: Data Privacy and Data Protection: US Law and Legislation4: Data Sovereignty: What It Is and Why It Matters

QUESTION 186
Which of the following is the BEST way to foster continuous improvement of IS audit processes and practices?

A. Invite external auditors and regulators to perform regular assessments of the IS audit function.
B. Implement rigorous managerial review and sign-off of IS audit deliverables.
C. Frequently review IS audit policies, procedures, and instruction manuals.
D. Establish and embed quality assurance (QA) within the IS audit function.

Correct Answer: D
Section:
Explanation:
The best way to foster continuous improvement of IS audit processes and practices is to establish and embed quality assurance (QA) within the IS audit function, as this will ensure that the IS audit activities are aligned with the standards, expectations, and objectives of the organization and the stakeholders12.QA involves periodic internal and external assessments, benchmarking, feedback, and root cause analysis to identify and address gaps, issues, and opportunities for improvement34.
Reference
1: The Basics and Principles of Continuous Improvement42: ISO 9001 Auditing Practices Group Guidance on53: INSIGHTS TO QUALITY34: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance2

QUESTION 187
Which of the following BEST indicates that the effectiveness of an organization's security awareness program has improved?

A. A decrease in the number of information security audit findings
B. An increase in the number of staff who complete awareness training
C. An increase in the number of phishing emails reported by employees
D. A decrease in the number of malware outbreaks

Correct Answer: C
Section:
Explanation:
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1.An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
Reference
1: The Importance Of Measuring Security Awareness2: Measuring the effectiveness of your security awareness program3: How effective is security awareness training?
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1.An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
Reference
1: The Importance Of Measuring Security Awareness2: Measuring the effectiveness of your security awareness program3: How effective is security awareness training?

QUESTION 188
Which of the following should be the GREATEST concern to an IS auditor reviewing the information security framework of an organization?

A. The information security policy has not been updated in the last two years.
B. Senior management was not involved in the development of the information security policy.
C. A list of critical information assets was not included in the information security policy.
D. The information security policy is not aligned with regulatory requirements.

Correct Answer: D
Section:
Explanation:

The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1.An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
Reference
1: The Importance Of Measuring Security Awareness2: Measuring the effectiveness of your security awareness program3: How effective is security awareness training?

QUESTION 189
An IS auditor finds that a recently deployed application has a number of developers with inappropriate update access left over from the testing environment. Which of the following would have BEST prevented the update access from being migrated?

A. Establishing a role-based matrix for provisioning users
B. Re-assigning user access rights in the quality assurance (QA) environment
C. Holding the application owner accountable for application security
D. Including a step within the system development life cycle (SDLC) to clean up access prior to go-live

Correct Answer: D
Section:

QUESTION 190
Which of the following is the MOST important consideration when developing tabletop exercises within a cybersecurity incident response plan?

A. Ensure participants are selected from all cross-functional units in the organization.
B. Create exercises that are challenging enough to prove inadequacies in the current incident response plan.
C. Ensure the incident response team will have enough distractions to simulate real-life situations.
D. Identify the scope and scenarios that are relevant to current threats faced by the organization.

Correct Answer: D
Section:
Explanation:
The most important consideration when developing tabletop exercises within a cybersecurity incident response plan is to identify the scope and scenarios that are relevant to current threats faced by the organization, as this will ensure that the exercises are realistic, meaningful, and effective in testing and improving the incident response capabilities12.The scope and scenarios should reflect the organization's risk profile, business objectives, and operational environment, and should cover a variety of potential incidents that could impact the organization's assets, operations, and reputation34.
Reference
1: Cybersecurity Incident Response Exercise Guidance - ISACA2: Cybersecurity Tabletop Exercises: Everything You Ever Wanted to Know3: CISA Tabletop Exercise Package4: Boost Your Incident Response Plan with Tabletop Exercises

QUESTION 191
In an annual audit cycle, the audit of an organization's IT department resulted in many findings. Which of the following would be the MOST important consideration when planning the next audit?

A. Postponing the review until all of the findings have been rectified
B. Limiting the review to the deficient areas
C. Verifying that all recommendations have been implemented
D. Following up on the status of all recommendations

Correct Answer: D
Section:
Explanation:
The most important consideration when planning the next audit after many findings is to follow up on the status of all recommendations, as this will ensure that the audit findings are addressed in a timely and effective

manner, and that the root causes of the issues are resolved12.Following up on the status of all recommendations will also help to assess the progress and performance of the IT department, and to identify any new or emerging risks or challenges34.
Reference
1: What to consider when resolving internal audit findings32: A brief guide to follow up43: Guidance on auditing planning for Internal Audit24: Corrective Action Plan (CAP): How to Manage Audit Findings1

QUESTION 192
An IS auditor would MOST likely recommend that IT management use a balanced scorecard to:

A. indicate whether the organization meets quality standards.
B. ensure that IT staff meet performance requirements.
C. train and educate IT staff.
D. assess IT functions and processes.

Correct Answer: D
Section:
Explanation:
A balanced scorecard is a strategic planning framework that companies use to assign priority to their products, projects, and services; communicate about their targets or goals; and plan their routine activities1. The scorecard enables companies to monitor and measure the success of their strategies to determine how well they have performed.A balanced scorecard for IT management can help assess IT functions and processes by defining four perspectives: financial, customer, internal business process, and learning and growth2.These perspectives can help IT management align their IT objectives with the organization's vision and mission, identify and prioritize the key performance indicators (KPIs) for IT, and evaluate the effectiveness and efficiency of IT operations and services3.
Reference
1: Balanced Scorecard - Overview, Four Perspectives2: The IT Balanced Scorecard (BSC) Explained - BMC Software3: A BALANCED SCORECARD (BSC) FOR IT PERFORMANCE MANAGEMENT - SAS Support

QUESTION 193
A sample for testing must include the 80 largest client balances and a random sample of the rest. What should the IS auditor recommend?

A. Query the database.
B. Develop an integrated test facility (ITF).
C. Use generalized audit software.
D. Leverage a random number generator.

Correct Answer: C
Section:
Explanation:
Generalized audit software is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases1.Generalized audit software can help the IS auditor to select a sample for testing that includes the 80 largest client balances and a random sample of the rest, by using functions such as sorting, filtering, stratifying, and randomizing the data23.Generalized audit software can also help the IS auditor to perform other audit procedures on the sample, such as verifying the accuracy, completeness, and validity of the data4.
Reference
1: Generalized Audit Software (GAS) - ISACA2: Audit Sampling - ISACA3: How to use generalized audit software to perform audit sampling4: Generalized Audit Software: A Review of Five Packages

QUESTION 194
Which of the following is the MOST appropriate testing approach when auditing a daily data flow between two systems via an automated interface to confirm that it is complete and accurate?

A. Confirm that the encryption standard applied to the interface is in line with best practice.
B. Inspect interface configurations and an example output of the systems.
C. Perform data reconciliation between the two systems for a sample of 25 days.
D. Conduct code review for both systems and inspect design documentation.

Correct Answer: C
Section:
Explanation:
The most appropriate testing approach when auditing a daily data flow between two systems via an automated interface is to perform data reconciliation between the two systems for a sample of 25 days.Data reconciliation is a process of verifying that the data transferred from one system to another is complete and accurate, and that there are no discrepancies or errors in the data flow1.Data reconciliation can be performed by using generalized audit software, which is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases2. By performing data reconciliation for a sample of 25 days, the IS auditor can test the reliability and consistency of the data flow over a reasonable period of time, and identify any potential issues or anomalies that could affect the quality of the data or the functionality of the systems.
Reference
1: Data Flow Testing - GeeksforGeeks2: Generalized Audit Software (GAS) - ISACA

QUESTION 195
In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the:

A. allocation of IT staff.
B. project management methodologies used.
C. major IT initiatives.
D. links to operational tactical plans.

Correct Answer: C
Section:
Explanation:
In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the major IT initiatives that are aligned with the organization's vision, mission, and objectives, and that support the business strategy and priorities12.The major IT initiatives should also be realistic, measurable, and achievable, and should have clear timelines, budgets, and responsibilities34.
Reference
1: IT Strategy Template for a Successful Strategic Plan | Gartner22: IT Strategy Template for a Successful Strategic Plan | Gartner43: Conduct a Strategic Plan Review & Assessment - Governance34: Time To Conduct A Strategy Review?Here's How To Get Started1

QUESTION 196
An IS auditor has been asked to review an event log aggregation system to ensure risk management practices have been applied. Which of the following should be of MOST concern to the auditor?

A. Log feeds are uploaded via batch process.
B. Completeness testing has not been performed on the log data.
C. The log data is not normalized.
D. Data encryption standards have not been considered.

Correct Answer: B
Section:
Explanation:
The IS auditor should be most concerned if completeness testing has not been performed on the log data, as this could indicate that some logs are missing, corrupted, or tampered with, and that the log aggregation system is not reliable or accurate12.Completeness testing is a process of verifying that all the logs generated by the source systems are successfully collected, transferred, and stored by the log aggregation system, and that there are no gaps or inconsistencies in the log data34. Completeness testing is essential for ensuring the integrity and validity of the log data, and for supporting the risk management practices of the organization.
Reference
1: Log Aggregation: How it Works, Methods, and Tools - Exabeam22: Log Aggregation & Monitoring Relation in Cybersecurity43: Log Aggregation: What It Is & How It Works | Datadog34: Data Flow Testing - GeeksforGeeks1

QUESTION 197
An IS auditor found that operations personnel failed to run a script contributing to year-end financial statements. Which of the following is the BEST recommendation?

A. Retrain operations personnel.
B. Implement a closing checklist.
C. Update the operations manual.
D. Bring staff with financial experience into operations.

Correct Answer: B
Section:
Explanation:
The best recommendation for the IS auditor to make is to implement a closing checklist, as this will help to ensure that all the required tasks and scripts are performed and verified during the year-end closing process12.A closing checklist can also help to prevent errors, omissions, and delays that could affect the accuracy and timeliness of the financial statements3.
Reference
1: Year-end closing procedures for GL - Dynamics GP | Microsoft Learn12: Year-end activities FAQ - Finance | Dynamics 365 | Microsoft Learn23: Year-End Closing Checklist: 10 Steps to Close Your Books3: Year End Closing Checklist: 7 Steps to Make it Easy

QUESTION 198
Which of the following is the GREATEST risk associated with security patches being automatically downloaded and applied to production servers?

A. Supporting documentation is not updated.
B. Anti-malware is disabled during patch installation.
C. Patches may be installed regardless of their criticality.
D. Patches may result in major service failures.

Correct Answer: D
Section:
Explanation:
The greatest risk associated with security patches being automatically downloaded and applied to production servers is that patches may result in major service failures, as they may introduce new bugs, conflicts, or incompatibilities that could affect the functionality, performance, or availability of the servers12.Automatic patching may also bypass the testing and validation processes that are necessary to ensure the quality and reliability of the patches34.
Reference
1: Do you leave Windows Automatic Updates enabled on your production IIS server?- Server Fault12: Azure now installs security updates on Windows VMs automatically33: Server Patch Management | Process of Server Patching - ManageEngine24: Windows Security Updates | Microsoft Patch Updates Guide - ManageEngine4

QUESTION 199
Effective separation of duties in an online environment can BEST be achieved by utilizing:

A. appropriate supervision.
B. transaction logging.
C. written procedure manuals.
D. access authorization tables.

Correct Answer: D
Section:
Explanation:
Access authorization tables are the best way to achieve effective separation of duties in an online environment, as they allow the definition and enforcement of different access rights and privileges for different users or roles, based on the principle of least privilege12.Access authorization tables can help to prevent unauthorized or inappropriate actions, such as fraud, errors, or misuse of the system, by ensuring that no user has enough privileges to perform all parts of a transaction or business process34.
Reference
1: Separation of Duty (SOD) - Glossary | CSRC32: Separation of Duties within Information Systems43: Separation of Duties: Implementation & Challenges in IT24: Implementing Segregation of Duties: A Practical Experience

QUESTION 200
From a risk management perspective, which of the following is the BEST approach when implementing a large and complex data center IT infrastructure?

A. Simulating the new infrastructure before deployment
B. Prototyping and a one-phase deployment
C. A deployment plan based on sequenced phases
D. A big bang deployment with a successful proof of concept

Correct Answer: C
Section:
Explanation:
The best approach from a risk management perspective when implementing a large and complex data center IT infrastructure is to use a deployment plan based on sequenced phases, as this will allow the organization to break down the project into manageable and measurable stages, and to monitor and control the progress, quality, and outcomes of each phase12.A phased deployment plan can also help to reduce the risks of errors, failures, or disruptions that could affect the entire infrastructure, and to implement corrective actions or contingency plans as needed34.
Reference
1: Data Center Project Planning: A Guide to Success22: Data Center Project Planning: A Guide to Success43: Data Center Migration: A Step-by-Step Guide34: Data Center Migration: A Step-by-Step Guide1

QUESTION 201
Which of the following is the BEST way to mitigate risk to an organization's network associated with devices permitted under a bring your own device (BYOD) policy?

A. Require personal devices to be reviewed by IT staff.
B. Enable port security on all network switches.
C. Implement a network access control system.
D. Ensure the policy requires antivirus software on devices.

Correct Answer: C
Section:
Explanation:
The best way to mitigate risk to an organization's network associated with devices permitted under a BYOD policy is to implement a network access control system, as this will allow the organization to monitor, authenticate, and authorize the devices that connect to the network, and to enforce security policies and compliance requirements12.A network access control system can help to prevent unauthorized or compromised devices from accessing sensitive data or resources, and to detect and isolate any potential threats or vulnerabilities34.
Reference
1: Network Access Control (NAC) - ISACA2: Network Access Control (NAC) - Cisco3: BYOD Security Risks: 6 Ways to Protect Your Organization - ReliaQuest54: How to Mitigate BYOD Risks and Challenges - CIOReview6

QUESTION 202
How does a continuous integration/continuous development (CI/CD) process help to reduce software failure risk?

A. Easy software version rollback
B. Smaller incremental changes
C. Fewer manual milestones
D. Automated software testing

Correct Answer: B
Section:
Explanation:
A continuous integration/continuous development (CI/CD) process helps to reduce software failure risk by enabling smaller incremental changes to the software code, rather than large and infrequent updates12.Smaller

incremental changes allow developers to detect and fix errors, bugs, or vulnerabilities more quickly and easily, and to ensure that the software is always in a working state34.Smaller incremental changes also reduce the complexity and uncertainty of the software development process, and improve the quality and reliability of the software product5.
Reference
1: What is CI/CD?Continuous integration and continuous delivery explained12: 5 CI/CD challenges---and how to solve them | TechBeacon43: Continuous Integration vs Continuous Delivery vs Continuous Deployment24: 7 CI/CD Challenges & their Must-Know Solutions | BrowserStack35: 5 common pitfalls of CI/CD---and how to avoid them | InfoWorld5

QUESTION 203
An IS auditor is reviewing an organization's incident management processes and procedures. Which of the following observations should be the auditor's GREATEST concern?

A. Ineffective post-incident review
B. Ineffective incident prioritization
C. Ineffective incident detection
D. Ineffective incident classification

Correct Answer: C
Section:

QUESTION 204
An IS auditor finds ad hoc vulnerability scanning is in place with no clear alignment to the organization's wider security threat and vulnerability management program.
Which of the following would BEST enable the organization to work toward improvement in this area?

A. Implementing security logging to enhance threat and vulnerability management
B. Maintaining a catalog of vulnerabilities that may impact mission-critical systems
C. Using a capability maturity model to identify a path to an optimized program
D. Outsourcing the threat and vulnerability management function to a third party

Correct Answer: C
Section:
Explanation:
The best way to enable the organization to work toward improvement in its security threat and vulnerability management program is to use a capability maturity model to identify a path to an optimized program.A capability maturity model is a framework that helps organizations assess their current level of performance and maturity in a specific domain, and provides guidance and best practices to achieve higher levels of excellence12.A capability maturity model for vulnerability management can help the organization to evaluate its current practices, identify gaps and weaknesses, and implement improvement actions based on the defined criteria and objectives34.
Reference
1: What is a Capability Maturity Model?12: Capability Maturity Model - Wikipedia23: Vulnerability Management Maturity Model - SANS Institute44: 5 Stages Of Vulnerability Management Maturity Model - SecPod Blog3

QUESTION 205
Which of the following controls is BEST implemented through system configuration?

A. Network user accounts for temporary workers expire after 90 days.
B. Application user access is reviewed every 180 days for appropriateness.
C. Financial data in key reports is traced to source systems for completeness and accuracy.
D. Computer operations personnel initiate batch processing jobs daily.

Correct Answer: A
Section:
Explanation:
This control is best implemented through system configuration because it can be enforced automatically by setting a parameter in the network operating system or directory service.This ensures that temporary workers do

not have access to the network beyond their authorized period, and reduces the risk of unauthorized or malicious use of their accounts12.
Reference 1: Configuration and Change Management - CISA 2: What is IT Governance? - Definition from Techopedia

QUESTION 206
The business case for an information system investment should be available for review until the:

A. information system investment is retired.
B. information system has reached end of life.
C. formal investment decision is approved.
D. benefits have been fully realized.

Correct Answer: D
Section:
Explanation:
The business case for an information system investment is a document that provides the rationale and justification for the investment, based on the expected costs, benefits, risks, and impacts of the project12.The business case should be available for review until the benefits have been fully realized, because it serves as a baseline for measuring the actual performance and outcomes of the project against the planned ones34.This helps to evaluate the success and value of the investment, and to identify any gaps or issues that need to be addressed5.
Reference
1: The Business Case for Security - CISA
2: Beyond the Business Case: New Approaches to IT Investment
3: #HowTo: Build a Business Case for Cybersecurity Investment
4: ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB
5: The Business Case for Security | CISA

QUESTION 207
Which of the following BEST demonstrates alignment of the IT department with the corporate mission?

A. Analysis of IT department functionality
B. Biweekly reporting to senior management
C. Annual board meetings
D. Quarterly steering committee meetings

Correct Answer: D
Section:
Explanation:
Quarterly steering committee meetings best demonstrate alignment of the IT department with the corporate mission because they provide a regular forum for strategic planning, decision making, and communication between IT leaders and business stakeholders12.Steering committee meetings help to ensure that IT goals and initiatives are aligned with the business vision, mission, and objectives, and that IT performance and value are monitored and evaluated34.
Reference
1: IT Governance and the Balanced Scorecard - ISACA Journal
2: IT Steering Committee Best Practices: A Recipe for Success
3: What is IT Governance?- Definition from Techopedia
4: CISA Cybersecurity Strategic Plan | CISA

QUESTION 208
An IS auditor noted a recent production incident in which a teller transaction system incorrectly charged fees to customers due to a defect from a recent release. Which of the following should be the auditor's NEXT step?

A. Evaluate developer training.

B. Evaluate the incident management process.
C. Evaluate the change management process.
D. Evaluate secure code practices.

Correct Answer: C
Section:
Explanation:
The change management process is the set of procedures and activities that ensure that changes to the information system are authorized, tested, documented, and implemented in a controlled manner12.A defect in a recent release indicates that there may be issues with the quality assurance, testing, or approval of the changes, which could affect the reliability, security, and performance of the system3. Therefore, the auditor's next step should be to evaluate the change management process and identify the root cause of the defect, as well as the impact and remediation of the incident.
Reference
1: Change Management - CISA
2: What is Change Management?- Definition from Techopedia
3: How to Audit Change Management - ISACA Journal
: The Business Case for Security | CISA

QUESTION 209
Which of the following is the PRIMARY reason for using a digital signature?

A. Provide availability to the transmission
B. Authenticate the sender of a message
C. Provide confidentiality to the transmission
D. Verify the integrity of the data and the identity of the recipient

Correct Answer: B
Section:
Explanation:
A digital signature is a mathematical algorithm that validates the authenticity and integrity of a message or document by generating a unique hash of the message or document and encrypting it using the sender's private key1.The primary reason for using a digital signature is to authenticate the sender of a message, as only the sender has access to their private key and can produce a valid signature2.A digital signature also verifies the integrity of the data, as any modification to the message or document will result in a different hash value and invalidate the signature1.However, a digital signature does not provide availability or confidentiality to the transmission, as it does not prevent denial-of-service attacks or encrypt the entire message or document3.
Reference
1: Understanding Digital Signatures | CISA
2: Signature Verification | CISA
3: SECFND: Digital Signatures from Skillsoft | NICCS

QUESTION 210
During an organization's implementation of a data loss prevention (DLP) solution, which of the following activities should be completed FIRST?

A. Configuring reports
B. Configuring rule sets
C. Enabling detection points
D. Establishing exceptions workflow

Correct Answer: B
Section:
Explanation:
Configuring rule sets is the first activity that should be completed during the implementation of a DLP solution, because rule sets define the criteria and actions for identifying, monitoring, and preventing data loss

incidents12.Rule sets are based on the organization's data classification, policies, and requirements, and they help to ensure that the DLP solution is aligned with the business objectives and risk appetite34.Configuring rule sets before enabling detection points, establishing exceptions workflow, or configuring reports helps to avoid false positives, false negatives, or unnecessary alerts5.
Reference
1: 3.13: Deploy a Data Loss Prevention Solution - Read the Docs
2: Plan and implement data loss prevention (DLP) [Guided] - NICCS
3: CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM DATA PROTECTION ... - CISA
4: Continuous Diagnostics and Mitigation Program Technical ... - CISA
5: Data Loss Prevention Best Practices - ISACA Journal

QUESTION 211
A new regulation has been enacted that mandates specific information security practices for the protection of customer data. Which of the following is MOST useful for an IS auditor to review when auditing against the regulation?

A. Compliance gap analysis
B. Customer data protection roles and responsibilities
C. Customer data flow diagram
D. Benchmarking studies of adaptation to the new regulation

Correct Answer: A
Section:
Explanation:
A compliance gap analysis is a detailed review of an organization's current state of compliance against a specific regulation or standard.It helps identify the areas and controls that are not meeting the requirements, assess their risk levels, and determine the corrective actions that can be taken to achieve compliance12. A compliance gap analysis is the most useful tool for an IS auditor to review when auditing against a new regulation, as it provides a clear and comprehensive picture of the compliance status, gaps, and remediation plan of the organization.
Reference
1: Information Security Architecture: Gap Assessment and Prioritization - ISACA
2: How to perform Compliance Gap Analysis? - Sprinto

QUESTION 212
An external attacker spoofing an internal Internet Protocol (IP) address can BEST be detected by which of the following?

A. Comparing the source address to the domain name server (DNS) entry
B. Using static IP addresses for identification
C. Comparing the source address to the interface used as the entry point
D. Using a state table to compare the message states of each packet as it enters the system

Correct Answer: D
Section:

QUESTION 213
During the audit of an enterprise resource planning (ERP) system, an IS auditor found an applicationpatch was applied to the production environment. It is MOST important for the IS auditor to verify approval from the:

A. information security officer.
B. system administrator.
C. information asset owner.
D. project manager.

Correct Answer: D
Section:

QUESTION 214
Which of the following would be of GREATEST concern to an IS auditor reviewing the feasibility study for a new application system?

A. Security requirements have not been defined.
B. Conditions under which the system will operate are unclear.
C. The business case does not include well-defined strategic benefits.
D. System requirements and expectations have not been clarified.

Correct Answer: D
Section:

QUESTION 215
When an intrusion into an organization's network is detected, which of the following should be done FIRST?

A. Notify senior management.
B. Block all compromised network nodes.
C. Identify nodes that have been compromised.
D. Contact law enforcement.

Correct Answer: D
Section:

QUESTION 216
Data from a system of sensors located outside of a network is received by the open ports on a server. Which of the following is the BEST way to ensure the integrity of the data being collected from the sensor system?

A. Implement network address translation on the sensor system.
B. Route the traffic from the sensor system through a proxy server.
C. Hash the data that is transmitted from the sensor system.
D. Transmit the sensor data via a virtual private network (VPN) to the server.

Correct Answer: D
Section:

QUESTION 217
Which of the following provides the BEST assurance that vendor-supported software remains up to date?

A. Release and patch management
B. Licensing agreement and escrow
C. Software asset management
D. Version management

Correct Answer: A
Section:

QUESTION 218
If a recent release of a program has to be backed out of production, the corresponding changes within the delta version of the code should be:

A. filed in production for future reference in researching the problem.
B. applied to the source code that reflects the version in production.
C. eliminated from the source code that reflects the version in production.
D. reinstalled when replacing the version back into production.

Correct Answer: C
Section:
Explanation:
When a program release needs to be backed out of production, the changes introduced by that release must be removed from the source code to ensure the system returns to its prior state. This approach ensures that the source code reflects the stable version without the problematic changes.
Reference
ISACA CISA Review Manual 27th Edition, Page 244-245 (Change Management)

QUESTION 219
A senior IS auditor suspects that a PC may have been used to perpetrate fraud in a finance department. The auditor should FIRST report this suspicion to:

A. the audit committee.
B. audit management.
C. auditee line management.
D. the police.

Correct Answer: B
Section:

QUESTION 220
Which of the following BEST describes the role of the IS auditor in a control self-assessment (CSA)?

A. Implementer
B. Facilitator
C. Approver
D. Reviewer

Correct Answer: B
Section:

QUESTION 221
An IS auditor is reviewing an organization that performs backups on local database servers every two weeks and does not have a formal policy to govern data backup and restoration procedures. Which of the following findings presents the GREATEST risk to the organization?

A. Lack of offsite data backups
B. Absence of a data backup policy
C. Lack of periodic data restoration testing
D. Insufficient data backup frequency

Correct Answer: D
Section:

QUESTION 222
An organization's information security policies should be developed PRIMARILY on the basis of:

A. enterprise architecture (EA).
B. industry best practices.
C. a risk management process.
D. past information security incidents.

Correct Answer: C
Section:

QUESTION 223
Which of the following BEST enables an IS auditor to confirm the batch processing to post transactions from an input source is successful?

A. Error log review
B. Total number of items
C. Hash totals
D. Aggregate monetary amount

Correct Answer: C
Section:

QUESTION 224
An organization's strategy to source certain IT functions from a Software as a Service (SaaS) provider should be approved by the:

A. chief financial officer (CFO).
B. chief risk officer (CRO).
C. IT steering committee.
D. IT operations manager.

Correct Answer: C
Section:

QUESTION 225
Which of the following should be the GREATEST concern for an IS auditor performing a post-implementation review for a major system upgrade?

A. Changes are promoted to production by the development group.
B. Object code can be accessed by the development group.
C. Developers have access to the testing environment.
D. Change approvals are not formally documented.

Correct Answer: D
Section:

QUESTION 226
An organization requires the use of a key card to enter its data center. Recently, a control was implemented that requires biometric authentication for each employee.
Which type of control has been added?

A. Corrective
B. Compensating
C. Preventive
D. Detective

Correct Answer: C
Section:

QUESTION 227
A steering committee established to oversee an organization's digital transformation program is MOSTlikely to be involved with which of the following activities?

A. Preparing project status reports
B. Designing interface controls
C. Reviewing escalated project issues
D. Documenting requirements

Correct Answer: C
Section:

QUESTION 228
Which of the following practices associated with capacity planning provides the GREATEST assurance that future incidents related to existing server performance will be prevented?

A. Reviewing results from simulated high-demand stress test scenarios
B. Performing a root cause analysis for past performance incidents
C. Anticipating current service level agreements (SLAs) will remain unchanged
D. Duplicating existing disk drive systems to improve redundancy and data storage

Correct Answer: A
Section:

QUESTION 229
Who is PRIMARILY responsible for the design of IT controls to meet control objectives?

A. Risk management
B. Business management
C. IT manager
D. Internal auditor

Correct Answer: C
Section:

QUESTION 230
Which of the following is MOST likely to be reduced when implementing optimal risk management strategies?

A. Sampling risk
B. Residual risk
C. Detection risk
D. Inherent risk

Correct Answer: D
Section:

QUESTION 231
Audit frameworks can assist the IS audit function by:

A. defining the authority and responsibility of the IS audit function.
B. providing direction and information regarding the performance of audits.
C. outlining the specific steps needed to complete audits.
D. providing details on how to execute the audit program.

Correct Answer: B
Section:

QUESTION 232
A current project to develop IT-based solutions will need additional funding to meet changes in business requirements. Who is BEST suited to obtain this additional funding?

A. Project sponsor
B. Project manager
C. IT strategy committee
D. Board of directors

Correct Answer: A
Section:

QUESTION 233
An IS auditor reviewing an information processing environment decides to conduct external penetration testing. Which of the following is MOST appropriate to include in the audit scope for the organization to distinguish between the auditor's penetration attacks and actual attacks?

A. Restricted host IP addresses of simulated attacks
B. Testing techniques of simulated attacks
C. Source IP addresses of simulated attacks
D. Timing of simulated attacks

Correct Answer: C
Section:

QUESTION 234
The PRIMARY role of an IS auditor in the remediation of problems found during an audit engagement is to:

A. help auditee management by providing the solution.

B. explain the findings and provide general advice.
C. present updated policies to management for approval.
D. take ownership of the problems and oversee remediation efforts.

Correct Answer: B
Section:

QUESTION 235
An IS auditor has been asked to review the quality of data in a general ledger system. Which of the following would provide the auditor with the MOST meaningful results?

A. Discussion of the largest account values with business owners
B. Integrity checks against source documentation
C. System vulnerability assessment
D. Interviews with system owners and operators

Correct Answer: B
Section:

QUESTION 236
An organization is establishing a steering committee for the implementation of a new enterprise resource planning (ERP) system that uses Agile project management methodology. What is the MOST important criterion for the makeup of this committee?

A. Senior management representation
B. Ability to meet the time commitment required
C. Agile project management experience
D. ERP implementation experience

Correct Answer: C
Section:

QUESTION 237
Which of the following would be MOST useful to an IS auditor when making recommendations to enable continual improvement of IT processes over time?

A. Benchmarking studies
B. Maturity model
C. IT risk register
D. IT incident log

Correct Answer: B
Section:

QUESTION 238
Following a merger, a review of an international organization determines the IT steering committee's decisions do not extend to regional offices as required in the consolidated IT operating model. Which of the following is the IS auditor's BEST recommendation?

A. Create regional centers of excellence.
B. Engage an IT governance consultant.

C. Create regional IT steering committees.
D. Update the IT steering committee's formal charter.

Correct Answer: D
Section:

QUESTION 239
While conducting a follow-up on an asset management audit, the IS auditor finds paid invoices for IT devices not recorded in the organization's inventory. Which of the following is the auditor's BEST course of action?

A. Ask the asset management staff where the devices are.
B. Alert both audit and operations management about the discrepancy.
C. Ignore the invoices since they are not part of the follow-up.
D. Make a note of the evidence to include it in the scope of a future audit.

Correct Answer: B
Section:

QUESTION 240
An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

A. Imported data is not disposed of frequently.
B. The transfer protocol is not encrypted.
C. The transfer protocol does not require authentication.
D. The quality of the data is not monitored.

Correct Answer: D
Section:

QUESTION 241
Who is accountable for an organization's enterprise risk management (ERM) program?

A. Board of directors
B. Steering committee
C. Chief risk officer (CRO)
D. Executive management

Correct Answer: A
Section:

QUESTION 242
Which of the following would be an IS auditor's BEST recommendation to senior management when several IT initiatives are found to be misaligned with the organization's strategy?

A. Define key performance indicators (KPIs) for IT.
B. Modify IT initiatives that do not map to business strategies.
C. Reassess the return on investment (ROI) for the IT initiatives.
D. Reassess IT initiatives that do not map to business strategies.

Correct Answer: D
Section:

QUESTION 243
Which of the following is the MOST effective way to evaluate the physical security of a data center?

A. Review data center access logs.
B. Interview data center stakeholders.
C. Review camera footage from the data center.
D. Perform a data center tour.

Correct Answer: D
Section:

QUESTION 244
Which of the following user actions poses the GREATEST risk for inadvertently introducing malware into a local network?

A. Uploading a file onto an internal server
B. Viewing a hypertext markup language (HTML) document
C. Downloading a file from an enterprise file share
D. Opening an email attachment from an external account

Correct Answer: D
Section:

QUESTION 245
Which of the following is the GREATEST risk if two users have concurrent access to the same database record?

A. Data integrity
B. Entity integrity
C. Referential integrity
D. Availability integrity

Correct Answer: A
Section:

QUESTION 246
Which of the following is the GREATEST concern related to an organization's data classification processes?

A. Users responsible for managing records are unaware of the data classification processes.
B. Systems used to manage the data classification processes are not synchronized.
C. The data classification processes have not been updated in the last year.
D. The data classification processes are not aligned with industry standards.

Correct Answer: A
Section:

QUESTION 247
An IS auditor learns that a business owner violated the organization's security policy by creating a web page with access to production data. The auditor's NEXT step should be to:

A. determine if sufficient access controls exist.
B. assess the sensitivity of the production data.
C. shut down the web page.
D. escalate to senior management.

Correct Answer: D
Section:

QUESTION 248
Which of the following should be the PRIMARY focus when communicating an IS audit issue to management?

A. The risk to which the organization is exposed due to the issue
B. The nature, extent, and timing of subsequent audit follow-up
C. How the issue was found and who bears responsibility
D. A detailed solution for resolving the issue

Correct Answer: A
Section:

QUESTION 249
A senior IS auditor suspects that a PC may have been used to perpetrate fraud in a finance department. The auditor should FIRST report this suspicion to:

A. the audit committee.
B. audit management.
C. auditee line management.
D. the police.

Correct Answer: B
Section:

QUESTION 250
When building or upgrading enterprise cryptographic infrastructure, which of the following is the MOST critical requirement for growing business environments?

A. Service discovery
B. Backup and restoration capabilities
C. Network throttling
D. Scalable architectures and systems

Correct Answer: D
Section:

QUESTION 251
Which of the following is the PRIMARY reason an IS auditor would recommend offsite backups although critical data is already on a redundant array of inexpensive disks (RAID)?

A. The array cannot offer protection against disk corruption.
B. The array cannot recover from a natural disaster.
C. The array relies on proper maintenance.
D. Disks of the array cannot be hot-swapped for quick recovery.

Correct Answer: B
Section:

QUESTION 252
Management has requested a post-implementation review of a newly implemented purchasing package to determine the extent that business requirements are being met. Which of the following is MOST likely to be assessed?

A. Acceptance testing results
B. Results of live processing
C. Implementation methodology
D. Purchasing guidelines and policies

Correct Answer: C
Section:

QUESTION 253
An organization requires the use of a key card to enter its data center. Recently, a control was implemented that requires biometric authentication for each employee. Which type of control has been added?

A. Detective
B. Preventive
C. Compensating
D. Corrective

Correct Answer: B
Section:

QUESTION 254
During which process is regression testing MOST commonly used?

A. System modification
B. Unit testing
C. Stress testing
D. Program development

Correct Answer: A
Section:

QUESTION 255
A review of IT interface controls finds an organization does not have a process to identify and correct records that do not get transferred to the receiving system. Which of the following is the IS auditor's BEST recommendation?

A. Enable automatic encryption, decryption, and electronic signing of data files.

B. Automate the transfer of data between systems as much as is feasible.
C. Have coders perform manual reconciliation of data between systems.D
D. Implement software to perform automatic reconciliations of data between systems.

Correct Answer: D
Section:

QUESTION 256
Which of the following should be of GREATEST concern to an IS auditor assessing the effectiveness of an organization's information security governance?

A. Risk assessments of information assets are not periodically performed.
B. All Control Panel Items
C. The information security policy does not extend to service providers.
D. There is no process to measure information security performance.
E. The information security policy is not reviewed by executive management.

Correct Answer: C
Section:

QUESTION 257
Which of the following can BEST reduce the impact of a long-term power failure?

A. Power conditioning unit
B. Emergency power-off switches
C. Battery bank
D. Redundant power source

Correct Answer: D
Section:

QUESTION 258
Which of the following findings would be of GREATEST concern when auditing an organization's end-user computing (EUC)?

A. Errors flowed through to financial statements
B. Reduced oversight by the IT department
C. Inconsistency of patching processes being followed
D. Inability to monitor EUC audit logs and activities

Correct Answer: C
Section:

QUESTION 259
Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

A. Perimeter firewall
B. Data loss prevention (DLP) system
C. Network segmentation

D. Web application firewall (WAF)

Correct Answer: C
Section:

QUESTION 260
Which of the following is an effective way to ensure the integrity of file transfers in a peer-to-peer (P2P) computing environment?

A. Associate a message authentication code with each file transferred.
B. Ensure the files are transferred through an intrusion detection system (IDS).
C. Encrypt the packets shared between peers within the environment.
D. Connect the client computers in the environment to a jump server.

Correct Answer: A
Section:

QUESTION 261
Which of the following criteria is MOST important for the successful delivery of benefits from an IT project?

A. Assessing the impact of changes to individuals and business units within the organization
B. Involving key stakeholders during the development and execution phases of the project
C. Ensuring that IT project managers have sign-off authority on the business case
D. Quantifying the size of the software development effort required by the project

Correct Answer: B
Section:

QUESTION 262
Which of the following tasks would cause the GREATEST segregation of duties (SoD) concern if performed by the person who reconciles the organization's device inventory?

A. Tracking devices used for spare parts
B. Creating the device policy
C. vIssuing devices to employees
D. Approving the issuing of devices

Correct Answer: C
Section:

QUESTION 263
An organization allows programmers to change production systems in emergency situations without seeking prior approval. Which of the following controls should an IS auditor consider MOST important?

A. Programmers' subsequent reports
B. Limited number of super users
C. Operator logs
D. Automated log of changes

Correct Answer: D
Section:

QUESTION 264
An IS auditor is reviewing documentation from a change that was applied to an application. Which of the following findings would be the GREATEST concern?

A. Testing documentation does not show manager approval.
B. Testing documentation is dated three weeks before the system implementation date.
C. Testing documentation is approved prior to completion of user acceptance testing (UAT).
D. Testing documentation is kept in hard copy format.

Correct Answer: C
Section:

QUESTION 265
A new system development project is running late against a critical implementation deadline. Which of the following is the MOST important activity?

A. Ensure that code has been reviewed.
B. Perform user acceptance testing (UAT).
C. Document last-minute enhancements.
D. Perform a pre-implementation audit.

Correct Answer: B
Section:

QUESTION 266
Which of the following BEST addresses the availability of an online store?

A. RAID level 5 storage devices
B. A mirrored site at another location
C. Online backups
D. Clustered architecture

Correct Answer: D
Section:

QUESTION 267
In order for a firewall to effectively protect a network against external attacks, what fundamental practice must be followed?

A. The firewall must be placed in the demilitarized zone (DMZ).
B. Only essential external services should be permitted.
C. Filters for external information must be defined.
D. All external communication must be via the firewall.

Correct Answer: B
Section:

QUESTION 268
What is the MOST effective way to manage contractors' access to a data center?

A. Badge identification worn by visitors
B. Escort requirement for visitor access
C. Management approval of visitor access
D. Verification of visitor identification

Correct Answer: B
Section:

QUESTION 269
Which of the following is the BEST way to strengthen the security of smart devices to prevent data leakage?

A. Enforce strong security settings on smart devices.
B. Require employees to formally acknowledge security procedures.
C. Review access logs to the organization's sensitive data in a timely manner.
D. Include usage restrictions in bring your own device (BYOD) security procedures.

Correct Answer: A
Section:

QUESTION 270
Which of the following is MOST important to define within a disaster recovery plan (DRP)?

A. A comprehensive list of disaster recovery scenarios and priorities
B. Business continuity plan (BCP)
C. Test results for backup data restoration
D. Roles and responsibilities for recovery team members

Correct Answer: D
Section:

QUESTION 271
When designing metrics for information security, the MOST important consideration is that the metrics:

A. conform to industry standards.
B. apply to all business units.
C. provide actionable data.
D. are easy to understand.

Correct Answer: C
Section:

QUESTION 272
Which of the following would be an IS auditor's BEST recommendation to senior management when several IT initiatives are found to be misaligned with the organization's strategy?

A. Modify IT initiatives that do not map to business strategies.
B. Reassess IT initiatives that do not map to business strategies.
C. Define key performance indicators (KPIs) for IT.
D. Reassess the return on investment (ROI) for the IT initiatives.

Correct Answer: B
Section:

QUESTION 273
During the planning phase of a data loss prevention (DLP) audit, management expresses a concern about mobile computing. Which of the following should the IS auditor identify as the associated risk?

A. Increased vulnerability due to anytime, anywhere accessibility
B. Increased need for user awareness training
C. The use of the cloud negatively impacting IT availability
D. Lack of governance and oversight for IT infrastructure and applications

Correct Answer: A
Section:

QUESTION 274
Which of the following is the BEST way to prevent social engineering incidents?

A. Ensure user workstations are running the most recent version of antivirus software.
B. Maintain an onboarding and annual security awareness program.
C. Include security responsibilities in job descriptions and require signed acknowledgment.
D. Enforce strict email security gateway controls.

Correct Answer: B
Section:

QUESTION 275
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

A. the organization's network.
B. the demilitarized zone (DMZ).
C. the Internet.
D. the organization's web server.

Correct Answer: C
Section:

QUESTION 276
Which of the following is the PRIMARY advantage of using an automated security log monitoring tool instead of conducting a manual review to monitor the use of privileged access?

A. Reduced costs associated with automating the review
B. Increased likelihood of detecting suspicious activity
C. Ease of storing and maintaining log file

D. Ease of log retrieval for audit purposes

Correct Answer: B
Section:

QUESTION 277
Which of the following is the PRIMARY reason an IS auditor would recommend offsite backups although critical data is already on a redundant array of inexpensive disks (RAID)?

A. Disks of the array cannot be hot-swapped for quick recovery.
B. The array cannot offer protection against disk corruption.
C. The array relies on proper maintenance.
D. The array cannot recover from a natural disaster.

Correct Answer: D
Section:

QUESTION 278
Which of the following should an IS auditor be MOST concerned with when a system uses RFID?

A. Scalability
B. Maintainability
C. Nonrepudiation
D. Privacy

Correct Answer: D
Section:

QUESTION 279
Which of the following components of a risk assessment is MOST helpful to management in determining the level of risk mitigation to apply?

A. Risk classification
B. Control self-assessment (CSA)
C. Risk identification
D. Impact assessment

Correct Answer: D
Section:

QUESTION 280
The waterfall life cycle model of software development is BEST suited for which of the following situations?

A. The project will involve the use of new technology.
B. The project intends to apply an object-oriented design approach.
C. The project requirements are well understood.
D. The project is subject to time pressures.

Correct Answer: C

Section:

QUESTION 281
Which of the following is the GREATEST risk related to the use of virtualized environments?

A. The host may be a potential single point of failure within the system.
B. There may be insufficient processing capacity to assign to guests.
C. There may be increased potential for session hijacking.
D. Ability to change operating systems may be limited.

Correct Answer: A
Section:

QUESTION 282
Which of the following cloud capabilities BEST enables an organization to meet unexpectedly high service demand?

A. Scalability
B. High availability
C. Alternate routing
D. Flexibility

Correct Answer: A
Section:

QUESTION 283
Which of the following is the MAIN risk associated with adding a new system functionality during the development phase without following a project change management process?

A. The project may go over budget.
B. The added functionality has not been documented.
C. The project may fail to meet the established deadline.
D. The new functionality may not meet requirements.

Correct Answer: D
Section:

QUESTION 284
An IS audit manager is preparing the staffing plan for an audit engagement of a cloud service provider. What should be the manager's PRIMARY concern when being made aware that a new auditor in the department previously worked for this provider?

A. Independence
B. Professional conduct
C. Subject matter expertise
D. Resource availability

Correct Answer: A
Section:

QUESTION 285
Which of the following is the PRIMARY purpose of a rollback plan for a system change?

A. To ensure steps exist to remove the change if necessary
B. To ensure testing can be re-performed if required
C. To ensure a backup exists before implementing a change
D. To ensure the system change is effective

Correct Answer: A
Section:

QUESTION 286
An IS auditor reviewing the system development life cycle (SDLC) finds there is no requirement for business cases. Which of the following should be offGREATEST concern to the organization?

A. Vendor selection criteria are not sufficiently evaluated.
B. Business resources have not been optimally assigned.
C. Business impacts of projects are not adequately analyzed.
D. Project costs exceed established budgets.

Correct Answer: B
Section:

QUESTION 287
Which of the following would be MOST useful to an IS auditor when making recommendations to enable continual improvement of IT processes over time?

A. IT incident log
B. Benchmarking studies
C. Maturity model
D. IT risk register

Correct Answer: B
Section:

QUESTION 288
What type of control has been implemented when secure code reviews are conducted as part of a deployment program?

A. Monitoring
B. Deterrent
C. Detective
D. Corrective

Correct Answer: C
Section:

QUESTION 289
Which of the following will provide the GREATEST assurance to IT management that a quality management system (QMS) is effective?

A. A high percentage of stakeholders satisfied with the quality of IT
B. A high percentage of IT processes reviewed by quality assurance (QA)
C. A high percentage of incidents being quickly resolved
D. A high percentage of IT employees attending quality training

Correct Answer: A
Section:

QUESTION 290
Which of the following types of firewalls provides the GREATEST degree of control against hacker intrusion?

A. Packet filtering router
B. Circuit gateway
C. Application-level gateway
D. Screening router.

Correct Answer: C
Section:

QUESTION 291
Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?

A. Information security policy
B. Industry standards
C. Incident response plan
D. Industry regulations

Correct Answer: D
Section:

QUESTION 292
Which of the following threats is mitigated by a firewall?

A. Intrusion attack
B. Asynchronous attack
C. Passive assault
D. Trojan horse

Correct Answer: A
Section:

QUESTION 293
Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

A. Alignment with an information security framework
B. Compliance with relevant regulations
C. Inclusion of mission and objectives

D. Consultation with security staff

Correct Answer: B
Section:

QUESTION 294
An IS auditor is reviewing a data conversion project. Which of the following is the auditor's BEST recommendation prior to go-live?

A. Conduct a mock conversion test.
B. Review test procedures and scenarios.
C. Automate the test scripts.
D. Establish a configuration baseline.

Correct Answer: A
Section:

QUESTION 295
A white box testing method is applicable with which of the following testing processes?

A. Integration testing
B. Parallel testing
C. Sociability testing
D. User acceptance testing (UAT)

Correct Answer: A
Section:

QUESTION 296
During a review, an IS auditor discovers that corporate users are able to access cloud-based applications and data from any Internet-connected web browser. Which of the following is the auditor's BEST recommendation to help prevent unauthorized access?

A. Utilize strong anti-malware controls on all computing devices.
B. Update security policies and procedures.
C. Implement an intrusion detection system (IDS).
D. Implement multi-factor authentication.

Correct Answer: D
Section:

QUESTION 297
Which of the following BEST indicates that an incident management process is effective?

A. Decreased number of calls to the help desk
B. Decreased time for incident resolution
C. Increased number of incidents reviewed by IT management
D. Increased number of reported critical incidents

Correct Answer: B
Section:

QUESTION 298
Which of the following BEST reflects a mature strategic planning process?

A. Action plans with IT requirements built into all projects
B. An IT strategic plan with specifications of controls and safeguards
C. An IT strategic plan that supports the corporate strategy
D. IT projects from the strategic plan are approved by management

Correct Answer: C
Section:

QUESTION 299
An IS audit team is evaluating documentation of the most recent application user access review. It is determined that the user list was not system generated. Which of the following should be of MOST concern?

A. Confidentiality of the user list
B. Timeliness of the user list review
C. Completeness of the user list
D. Availability of the user list

Correct Answer: C
Section:

QUESTION 300
An incident response team has been notified of a virus outbreak in a network subnet. Which of the following should be the NEXT step?

A. Focus on limiting the damage.
B. Remove and restore the affected systems.
C. Verify that the compromised systems are fully functional.
D. Document the incident.

Correct Answer: A
Section:

QUESTION 301
Which of the following should be the GREATEST concern to an IS auditor reviewing an organization's job scheduling practices?

A. Most jobs are run manually.
B. Jobs are executed during working hours.
C. Job dependencies are undefined.
D. Job processing procedures are missing.

Correct Answer: C
Section:

QUESTION 302
Which of the following is the GREATEST impact as a result of the ongoing deterioration of a detective control?

A. Decreased effectiveness of root cause analysis
B. Decreased overall recovery time
C. Increased number of false negatives in security logs
D. Increased demand for storage space for logs

Correct Answer: C
Section:

QUESTION 303
Which of the following is the BEST way to ensure a vendor complies with system security requirements?

A. Require security training for vendor staff.
B. Review past incidents reported by the vendor.
C. Review past audits on the vendor's security compliance.
D. Require a compliance clause in the vendor contract.

Correct Answer: D
Section:

QUESTION 304
What is the PRIMARY reason to adopt a risk-based IS audit strategy?

A. To achieve synergy between audit and other risk management functions
B. To prioritize available resources and focus on areas with significant risk
C. To reduce the time and effort needed to perform a full audit cycle
D. To identify key threats, risks, and controls for the organization

Correct Answer: B
Section:

QUESTION 305
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

A. Risk acceptance
B. Risk transfer
C. Risk reduction
D. Risk avoidance

Correct Answer: D
Section:

QUESTION 306
Which of the following constitutes an effective detective control in a distributed processing environment?

A. A log of privileged account use is reviewed.
B. A disaster recovery plan (DRP)4% in place for the entire system.
C. User IDs are suspended after three incorrect passwords have been entered.
D. Users are required to request additional access via an electronic mail system.

Correct Answer: A
Section:

QUESTION 307
Which of the following is the BEST disposal method for flash drives that previously stored confidential data?

A. Destruction
B. Degaussing
C. Cryptographic erasure
D. Overwriting

Correct Answer: A
Section:

QUESTION 308
During a follow-up engagement, an IS auditor confirms evidence of a problem that was not an issue in the original audit. Which of the following is the auditor's BEST course of action?

A. Include the evidence as part of a future audit.
B. Report only on the areas within the scope of the follow-up.
C. Report the risk to management in the follow-up report.
D. Expand the follow-up scope to include examining the evidence.

Correct Answer: C
Section:

QUESTION 309
What should be the PRIMARY focus during a review of a business process improvement project?

A. Business project plan
B. Continuous monitoring plans
C. The cost of new controls
D. Business impact

Correct Answer: D
Section:

QUESTION 310
Which of the following is MOST important to the effectiveness of smoke detectors installed in a data processing facility?

A. Detectors trigger audible alarms when activated.
B. Detectors have the correct industry certification.

C. Detectors are linked to dry pipe fire suppression systems.
D. Detectors are linked to wet pipe fire suppression systems.

Correct Answer: A
Section:

QUESTION 311
Which of the following BEST indicates a need to review an organization's information security policy?

A. High number of low-risk findings in the audit report
B. Increasing exceptions approved by management
C. Increasing complexity of business transactions
D. Completion of annual IT risk assessment

Correct Answer: B
Section:

QUESTION 312
An IS auditor is evaluating the log management system for an organization with devices and systems in multiple geographic locations. Which of the following is MOST important for the auditor to verify?

A. Log files are reviewed in multiple locations.
B. Log files are concurrently updated.
C. Log files are encrypted and digitally signed.
D. Log files of the servers are synchronized.

Correct Answer: C
Section:

QUESTION 313
An organization is ready to implement a new IT solution consisting of multiple modules. The last module updates the processed data into the database. Which of the following findings should be of MOST concern to the IS auditor?

A. Absence of a formal change approval process
B. Lack of input validation
C. Use of weak encryption
D. Lack of a data dictionary

Correct Answer: B
Section:

QUESTION 314
Which of the following observations regarding change management should be considered the MOST serious risk by an IS auditor?

A. There is no software used to track change management.
B. The change is not approved by the business owners.
C. The change is deployed two weeks after approval.
D. The development of the change is not cost-effective.

Correct Answer: B
Section:

QUESTION 315
Which of the following is MOST important when creating a forensic image of a hard drive?

A. Requiring an independent third party be present while imaging
B. Securing a backup copy of the hard drive
C. Generating a content hash of the hard drive
D. Choosing an industry-leading forensics software tool

Correct Answer: C
Section:

QUESTION 316
Which of the following is the MOST efficient control to reduce the risk associated with a systems administrator having network administrator responsibilities?

A. The administrator must obtain temporary access to make critical changes.
B. The administrator will need to request additional approval for critical changes.
C. The administrator must sign a due diligence agreement.
D. The administrator will be subject to unannounced audits.

Correct Answer: B
Section:

QUESTION 317
A web application is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

A. Web application firewall (WAF) implementation
B. Penetration test results
C. Code review by a third party
D. Database application monitoring logs

Correct Answer: B
Section:

QUESTION 318
Which of the following is the GREATEST benefit of adopting an Agile audit methodology?

A. Better ability to address key risks
B. Less frequent client interaction
C. Annual cost savings
D. Reduced documentation requirements

Correct Answer: A
Section:

QUESTION 319
The PRIMARY objective of a follow-up audit is to:

A. assess the appropriateness of recommendations.
B. verify compliance with policies.
C. evaluate whether the risk profile has changed.
D. determine adequacy of actions taken on recommendations.

Correct Answer: D
Section:

QUESTION 320
An IS auditor can BEST evaluate the business impact of system failures by:

A. assessing user satisfaction levels.
B. interviewing the security administrator.
C. analyzing equipment maintenance logs.
D. reviewing system-generated logs.

Correct Answer: A
Section:

QUESTION 321
Which of the following is a threat to IS auditor independence?

A. Internal auditors share the audit plan and control test plans with management prior to audit commencement.
B. Internal auditors design remediation plans to address control gaps identified by internal audit.
C. Internal auditors attend IT steering committee meetings.
D. Internal auditors recommend appropriate controls for systems in development.

Correct Answer: B
Section:

QUESTION 322
Which of the following findings related to segregation of duties should be of GREATEST concern to an IS auditor?

A. The person who tests source code also approves changes.
B. The person who administers servers is also part of the infrastructure management team.
C. The person who creates new user accounts also modifies user access levels.
D. The person who edits source code also has write access to production.

Correct Answer: D
Section:

QUESTION 323
When reviewing hard disk utilization reports, an IS auditor observes that utilization is routinely above 95%. Which of the following should be the GREATEST concern to the IS auditor?

A. Availability
B. Consistency
C. Denial of service (DoS) attacks
D. Data security

Correct Answer: A
Section:

QUESTION 324
Which of the following would be of GREATEST concern to an IS auditor reviewing an IT-related customer service project?

A. The project risk exceeds the organization's risk appetite.
B. Executing the project will require additional investments.
C. Expected business value is expressed in qualitative terms.
D. The organization will be the first to offer the proposed services.

Correct Answer: A
Section:

QUESTION 325
An IS auditor discovers that a developer has used the same key to grant access to multiple applications making calls to an application programming interface (API). Which of the following is the BEST recommendation to address this situation?

A. Replace the API key with time-limited tokens that grant least privilege access.
B. Authorize the API key to allow read-only access by all applications.
C. Implement a process to expire the API key after a previously agreed-upon period of time.
D. Coordinate an API key rotation exercise with all impacted application owners.

Correct Answer: A
Section:

QUESTION 326
In an area susceptible to unexpected increases in electrical power, which of the following would MOST effectively protect the system?

A. Generator
B. Voltage regulator
C. Circuit breaker
D. Alternate power supply line

Correct Answer: B
Section:

QUESTION 327
An organization plans to centrally decommission end-of-life databases and migrate the data to the latest model of hardware. Which of the following BEST ensures data integrity is preserved during the migration?

A. Reconciling sample data to most recent backups
B. Obfuscating confidential data

C. Encrypting the data
D. Comparing checksums

Correct Answer: D
Section:

QUESTION 328
During a closing meeting, the IT manager disagrees with a valid audit finding presented by the IS auditor and requests the finding be excluded from the final report. Which of the following is the auditor's BEST course of action?

A. Request that the IT manager be removed from the remaining meetings and future audits.
B. Modify the finding to include the IT manager's comments and inform the audit manager of the changes.
C. Remove the finding from the report and continue presenting the remaining findings.
D. Provide the evidence which supports the finding and keep the finding in the report.

Correct Answer: D
Section:

QUESTION 329
During which IT project phase is it MOST appropriate to conduct a benefits realization analysis?

A. Post-implementation review phase
B. Final implementation phase
C. User acceptance testing (UAT) phase
D. Design review phase

Correct Answer: A
Section:

QUESTION 330
When planning a review of IT governance, an IS auditor is MOST likely to:

A. assess whether business process owner responsibilities are consistent.
B. obtain information about the control framework adopted by management.
C. examine audit committee minutes for IT-related controls.
D. define key performance indicators (KPIs).

Correct Answer: B
Section:

QUESTION 331
Which of the following is the BEST indicator that a third-party vendor adheres to the controls required by the organization?

A. Review of monthly performance reports submitted by the vendor
B. Certifications maintained by the vendor
C. Regular independent assessment of the vendor
D. Substantive log file review of the vendor's system

Correct Answer: C
Section:

QUESTION 332
Which of the following would BEST prevent an arbitrary application of a patch?

A. Database access control
B. Established maintenance windows
C. Network based access controls
D. Change management

Correct Answer: D
Section:

QUESTION 333
Which of the following would be MOST important to include in an IS audit report?

A. Observations not reported as findings due to inadequate evidence
B. The roadmap for addressing the various risk areas
C. The level of unmitigated risk along with business impact
D. Specific technology solutions for each audit observation

Correct Answer: C
Section:

QUESTION 334
At the end of each business day, a business-critical application generates a report of financial transac-tions greater than a certain value, and an employee then checks these transactions for errors. What type of control is in place?

A. Detective
B. Preventive
C. Corrective
D. Deterrent

Correct Answer: A
Section:

QUESTION 335
An organization has implemented a new data classification scheme and asks the IS auditor to evaluate its effectiveness. Which of the following would be of GREATEST concern to the auditor?

A. End-user managers determine who should access what information.
B. The organization has created a dozen different classification categories.
C. The compliance manager decides how the information should be classified.
D. The organization classifies most of its information as confidential.

Correct Answer: D

Section:

QUESTION 336
In a data center audit, an IS auditor finds that the humidity level is very low. The IS auditor would be MOST concerned because of an expected increase in:

A. risk of fire.
B. backup tape failures.
C. static electricity problems.
D. employee discomfort.

Correct Answer: C
Section:

QUESTION 337
An organization's business continuity plan (BCP) should be:

A. updated before an independent audit review.
B. tested after an intrusion attempt into the organization's hot site.
C. tested whenever new applications are implemented.
D. updated based on changes to personnel and environments.

Correct Answer: D
Section:
Explanation:
A BCP must stay current with organizational changes to ensure its effectiveness during a disruption. Personnel changes and environmental updates are directly relevant to how the BCP would be executed.
Reference
ISACA CISA Review Manual (Current Edition)- Chapter on Business Continuity and Disaster Recovery
Industry Standards (e.g., ISO 22301, NIST SP 800-34)- Guidelines for maintaining and updating a Business Continuity Plan

QUESTION 338
Which of the following presents the GREATEST risk associated with end-user computing (EUC) applica-tions over financial reporting?

A. Inability to quickly modify and deploy a solution
B. Lack of portability for users
C. Loss of time due to manual processes
D. Calculation errors in spreadsheets

Correct Answer: D
Section:
Explanation:
Spreadsheets, often used in EUC, are prone to manual input errors and formula mistakes. These errors can significantly compromise the accuracy and integrity of financial reporting.
Reference
ISACA CISA Review Manual (Current Edition)- Chapter on End-User Computing (EUC) risks
Industry Research on Spreadsheet Errors:Multiple studies highlight the prevalence of errors in spreadsheets, especially those used for financial purposes.

QUESTION 339
As part of an audit response, an auditee has concerns with the recommendations and is hesitant to implement them. Which of the following is the BEST course of action for the IS auditor?

A. Accept the auditee's response and perform additional testing.
B. Suggest hiring a third-party consultant to perform a current state assessment.
C. Conduct further discussions with the auditee to develop a mitigation plan.
D. Issue a final report without including the opinion of the auditee.

Correct Answer: C
Section:
Explanation:
Collaborative discussions help address the auditee's concerns, find mutually agreeable solutions, and create buy-in for implementing improvements.
Reference
ISACA CISA Review Manual (Current Edition)- Chapters on audit reporting and communication
Auditing Standards- Emphasize the importance of understanding and addressing auditee concerns.

QUESTION 340
Following an IT audit, management has decided to accept the risk highlighted in the audit report. Which of the following would provide the MOST assurance to the IS auditor that management is adequately balancing the needs of the business with the need to manage risk?

A. A communication plan exists for informing parties impacted by the risk.
B. Potential impact and likelihood are adequately documented.
C. Identified risk is reported into the organization's risk committee.
D. Established criteria exist for accepting and approving risk.

Correct Answer: D
Section:
Explanation:
Clear criteria ensure a consistent, rational approach to risk acceptance decisions, demonstrating management's deliberate and informed approach to risk management.
Reference
ISACA CISA Review Manual (Current Edition)- Chapter on Risk Management
Risk Management Frameworks (e.g., ISO 31000, NIST SP 800-39)- Emphasize the importance of defined risk assessment and decision-making processes.

QUESTION 341
During an information security review, an IS auditor learns an organizational policy requires all employ-ees to attend information security training during the first week of each new year. What is the auditor's BEST recommendation to ensure employees hired after January receive adequate guid-ance regarding security awareness?

A. Ensure new employees read and sign acknowledgment of the acceptable use policy.
B. Revise the policy to include security training during onboarding.
C. Revise the policy to require security training every six months for all employees.
D. Require management of new employees to provide an overview of security awareness.

Correct Answer: B
Section:
Explanation:
This directly addresses the gap for new hires, creates a consistent expectation regardless of hiring date, and formalizes the process within organizational policy.
Reference
ISACA CISA Review Manual (Current Edition)- Chapters on Information Security Policies, Training and Awareness
Industry Best Practices for Security Awareness- Emphasize the importance of timely and comprehensive training for new employees.

QUESTION 342

Which of the following procedures for testing a disaster recovery plan (DRP) is MOST effective?

A. Testing at a secondary site using offsite data backups
B. Performing a quarterly tabletop exercise
C. Reviewing recovery time and recovery point objectives
D. Reviewing documented backup and recovery procedures

Correct Answer: A
Section:

QUESTION 343
An IS auditor is tasked to review an organization's plan-do-check-act (PDCA) method for improving IT-related processes and wants to determine the accuracy of defined targets to be achieved. Which of the following steps in the PDCA process should the auditor PRIMARILY focus on in this situation?

A. Check
B. Plan
C. Do
D. Act

Correct Answer: B
Section:
Explanation:
In the PDCA cycle, the 'Plan' phase is where targets and objectives are defined. Focusing on this phase allows the auditor to evaluate the accuracy and appropriateness of the defined targets before they are implemented and measured in subsequent phases.
Reference
ISACA CISA Review Manual 27th Edition, Page 315-316 (PDCA Cycle)

QUESTION 344
Which of the following should be used as the PRIMARY basis for prioritizing IT projects and initiatives?

A. Estimated cost and time
B. Level of risk reduction
C. Expected business value
D. Available resources

Correct Answer: C
Section:

QUESTION 345
Which of the following network communication protocols is used by network devices such as routers to send error messages and operational information indicating success or failure when communicating with another IP address?

A. Transmission Control Protocol/Internet Protocol (TCP/IP)
B. Internet Control Message Protocol
C. Multipurpose Transaction Protocol
D. Point-to-Point Tunneling Protocol

Correct Answer: B
Section:

QUESTION 346
An IS auditor reviewing an organization's IT systems finds that the organization frequently purchases systems that are incompatible with the technologies already in the organization. Which of the following is the MOST likely reason?

A. Ineffective risk management policy
B. Lack of enterprise architecture (EA)
C. Lack of a maturity model
D. Outdated enterprise resource planning (ERP) system

Correct Answer: B
Section:

QUESTION 347
An IS auditor discovers that backups of critical systems are not being performed in accordance with the recovery point objective (RPO) established in the business continuity plan (BCP). What should the auditor do NEXT?

A. Request an immediate backup be performed.
B. Expand the audit scope.
C. Identify the root cause.
D. Include the observation in the report.

Correct Answer: B
Section:

QUESTION 348
A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

A. Business objectives
B. Business impact analysis (BIA)
C. Enterprise architecture (EA)
D. Recent incident trends

Correct Answer: A
Section:

QUESTION 349
An IS auditor wants to gain a better understanding of an organization's selected IT operating system software. Which of the following would be MOST helpful to review?

A. Service level agreements (SLAs)
B. Project steering committee charter
C. IT audit reports
D. Enterprise architecture (EA)

Correct Answer: C
Section:

QUESTION 350
Which of the following should be the PRIMARY consideration when validating a data analytic algorithm that has never been used before?

A. Enhancing the design of data visualization
B. Increasing speed and efficiency of audit procedures
C. Confirming completeness and accuracy
D. Decreasing the time for data analytics execution

Correct Answer: C
Section:

QUESTION 351
Which of the following findings would be of GREATEST concern to an IS auditor reviewing the security architecture of an organization that has just implemented a Zero Trust solution?

A. An increase in security-related costs
B. User complaints about the new mode of working
C. An increase in user identification errors
D. A noticeable drop in the performance of IT systems

Correct Answer: C
Section:

QUESTION 352
Which of the following staff should an IS auditor interview FIRST to obtain a general overview of the various technologies used across different programs?

A. Technical architect
B. Enterprise architect
C. Program manager
D. Solution architect

Correct Answer: B
Section:

QUESTION 353
A mission-critical application utilizes a one-node database server. On multiple occasions, the database service has been stopped to perform routine patching, causing application outages. Which of the following should be the IS auditor's GREATEST concern?

A. Revenue lost due to application outages
B. Patching performed by the vendor
C. A large number of scheduled database changes
D. The presence of a single point of failure

Correct Answer: D
Section:

QUESTION 354
A system performance dashboard indicates several application servers are reaching the defined threshold for maximum CPU allocation. Which of the following would be the IS auditor's BEST recommendation for the IT

department?

A. Increase the defined processing threshold to reflect capacity consumption during normal operations.
B. Notify end users of potential disruptions caused by degradation of servers.
C. Terminate both ingress and egress connections of these servers to avoid overload.
D. Validate the processing capacity of these servers is adequate to complete computing tasks.

Correct Answer: D
Section:

QUESTION 355
Which of the following controls helps to ensure that data extraction queries run by the database administrator (DBA) are monitored?

A. Restricting access to DBA activities
B. Performing periodic access reviews
C. Storing logs of database access
D. Reviewing activity logs of the DBA

Correct Answer: D
Section:

QUESTION 356
When protecting the confidentiality of information assets, the MOST effective control practice is the:

A. Awareness training of personnel on regulatory requirements
B. Utilization of a dual-factor authentication mechanism
C. Configuration of read-only access to all users
D. Enforcement of a need-to-know access control philosophy

Correct Answer: D
Section:

QUESTION 357
Which of the following is the MOST important consideration when establishing operational log management?

A. Types of data
B. Log processing efficiency
C. IT organizational structure
D. Log retention period

Correct Answer: D
Section:

QUESTION 358
An IS auditor is reviewing a machine learning model that predicts the likelihood that a user will watch a certain movie. Which of the following would be of GREATEST concern to the auditor?

A. When the model was tested with data drawn from a different population, the accuracy decreased.

B. The data set for training the model was obtained from an unreliable source.
C. An open-source programming language was used to develop the model.
D. The model was tested with data drawn from the same population as the training data.

Correct Answer: B
Section:

QUESTION 359
Which of the following poses the GREATEST risk to the use of active RFID tags?

A. Session hijacking
B. Eavesdropping
C. Piggybacking
D. Phishing attacks

Correct Answer: B
Section:

QUESTION 360
Which of the following should be of MOST concern to an IS auditor reviewing an organization's operational log management?

A. Log file size has grown year over year.
B. Critical events are being logged to immutable log files.
C. Applications are logging events into multiple log files.
D. Data formats have not been standardized across all logs.

Correct Answer: D
Section:

QUESTION 361
An IS auditor is reviewing a medical device that is attached to a patient's body, which automatically takes and uploads measurements to a cloud server. Treatment may be updated based on the measurements. Which of the following should be the auditor's PRIMARY focus?

A. Physical access controls on the device
B. Security and quality certification of the device
C. Device identification and authentication
D. Confirmation that the device is regularly updated

Correct Answer: B
Section:

QUESTION 362
An organization offers an e-commerce platform that allows consumer-to-consumer transactions. The platform now uses blockchain technology to ensure the parties are unable to deny the transactions. Which of the following attributes BEST describes the risk element that this technology is addressing?

A. Integrity
B. Nonrepudiation

C. Confidentiality
D. Availability

Correct Answer: B
Section:

QUESTION 363
Which of the following should be an IS auditor's PRIMARY focus when auditing the implementation of a new IT operations performance monitoring system?

A. Reviewing whether all changes have been implemented
B. Validating whether baselines have been established
C. Confirming whether multi-factor authentication (MFA) is deployed as part of the operational enhancements
D. Determining whether there is a process for annual review of the maintenance manual

Correct Answer: B
Section:

QUESTION 364
A startup organization wants to develop a data loss prevention (DLP) program. The FIRST step should be to implement:

A. Security awareness training
B. Data encryption
C. Data classification
D. Access controls

Correct Answer: C
Section: