Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (Topic 3)
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.

Answer: A

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. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

NEW QUESTION 2
- (Topic 3)
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.

Answer: D

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

NEW QUESTION 3
- (Topic 3)
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.

Answer: B

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. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 374

NEW QUESTION 4
- (Topic 3)
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.

Answer: D

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. References: 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 …

NEW QUESTION 5
- (Topic 3)
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

Answer: D

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. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 64

NEW QUESTION 6
- (Topic 3)
A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an application developer?

A. IT operator
B. System administration
C. Emergency support
D. Database administration

Answer: C

Explanation:
Segregation of duties (SOD) is a core internal control and an essential component of an effective risk management strategy. SOD emphasizes sharing the responsibilities of key business processes by distributing the discrete functions of these processes to multiple people and departments, helping to reduce the risk of possible errors and fraud1.
SOD is especially important in IT security, where granting excessive system access to one person or group can lead to harmful consequences, such as data breaches, identity theft, or bypassing security controls2. SOD breaks IT-related tasks into four separate function categories: authorization, custody, recordkeeping, and reconciliation1. Ideally, no one person or department holds responsibility in multiple categories.
In a role-based environment, where access privileges are granted based on predefined roles, it is important to ensure that the roles are designed and assigned in a way that supports SOD. For example, the person who develops an application should not also be the one who tests it, deploys it, or maintains it.
Therefore, an application developer should not be assigned the roles of IT operator, system administration, or database administration, as these roles may conflict with their development role and create opportunities for misuse or abuse of the system. The only role that may be assigned to an application developer without violating SOD is emergency support, which is a temporary role that allows the developer to access the system in case of a critical issue that requires immediate resolution3. However, even this role should be granted with caution and monitored closely to ensure compliance with SOD policies. References:
? ISACA, CISA Review Manual, 27th Edition, 2019, page 2824
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066692
? Hyperproof Blog, Segregation of Duties: What it is and Why it's Important1
? Advisera Blog, Segregation of duties in your ISMS according to ISO 27001A.6.1.23

NEW QUESTION 7
- (Topic 3)
What Is the BEST method to determine if IT resource spending is aligned with planned project spending?

A. Earned value analysis (EVA)
B. Return on investment (ROI) analysis
C. Gantt chart
D. Critical path analysis

Answer: A

Explanation:
The best method to determine if IT resource spending is aligned with planned project spending is earned value analysis (EVA). EVA is a technique that compares the actual cost, schedule, and scope of a project with the planned or budgeted values. EVA can help to measure the project progress and performance, and identify any variances or deviations from the baseline plan1.
EVA uses three basic values to calculate the project status: planned value (PV), earned value (EV), and actual cost (AC). PV is the amount of work that was expected to be completed by a certain date, according to the project plan. EV is the amount of work that was actually completed by that date, measured in terms of the budgeted cost. AC is the amount of money that was actually spent to complete the work by that date1.
By comparing these values, EVA can determine if the project is on track, ahead, or behind schedule and budget. EVA can also calculate various indicators, such as cost variance (CV), schedule variance (SV), cost performance index (CPI), and schedule performance index (SPI), to quantify the magnitude and direction of the variances. EVA can also forecast the future performance and completion of the project, based on the current trends and assumptions1.
The other options are not as effective as EVA in determining if IT resource spending is aligned with planned project spending. Option B, return on investment (ROI) analysis, is a technique that evaluates the profitability or efficiency of an investment, by comparing the benefits or revenues with the costs. ROI analysis can help to justify or prioritize a project, but it does not measure the actual progress or performance of the project against the plan2. Option C, Gantt chart, is a tool that displays the tasks, durations, dependencies, and milestones of a project in a graphical format. Gantt chart can help to plan and monitor a project schedule, but it does not show the actual cost or scope of the project3. Option D, critical path analysis, is a technique that identifies the longest sequence of tasks or activities that must be completed on time for the project to finish on schedule. Critical path analysis can help to optimize and control a project schedule, but it does not account for the actual cost or scope of the project4.
References:
? Earned Value Analysis & Management (EVA/EVM) – Definition & Formulae1
? Return on Investment (ROI) Formula2
? What Is a Gantt Chart?3
? Critical Path Method for Project Management

NEW QUESTION 8
- (Topic 3)
In response to an audit finding regarding a payroll application, management implemented a new automated control. Which of the following would be MOST helpful to the IS auditor when evaluating the effectiveness of the new control?

A. Approved test scripts and results prior to implementation
B. Written procedures defining processes and controls
C. Approved project scope document
D. A review of tabletop exercise results

Answer: B

Explanation:
The best way to evaluate the effectiveness of a new automated control is to review the written procedures that define the processes and controls. This will help the IS auditor to understand the objectives, scope, roles, responsibilities, and expected outcomes of the control. The written procedures will also provide a basis for testing the control and verifying its compliance with the audit finding recommendations. References:
? ISACA Frameworks: Blueprints for Success
? CISA Review Manual (Digital Version)

NEW QUESTION 9
- (Topic 3)
Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

A. Rotating backup copies of transaction files offsite
B. Using a database management system (DBMS) to dynamically back-out partially processed transactions
C. Maintaining system console logs in electronic formal
D. Ensuring bisynchronous capabilities on all transmission lines

Answer: B

Explanation:
The best way to ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure is to use a database management system (DBMS) to dynamically back-out partially processed transactions. A DBMS is a software system that manages the creation, manipulation, retrieval, and security of data stored in a database. A DBMS can provide features such as transaction management, concurrency control, recovery management, and integrity management. A DBMS can dynamically back-out partially processed transactions by using mechanisms such as rollback segments, undo logs, or write-ahead logs. These mechanisms allow the DBMS to restore the database to a consistent state before the failure occurred.
References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 10
- (Topic 3)
During a security audit, an IS auditor is tasked with reviewing log entries obtained from an enterprise intrusion prevention system (IPS). Which type of risk would be associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration?

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

Answer: B

Explanation:
The type of risk associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration is detection

risk. Detection risk is the risk that the auditor's procedures will not detect a material misstatement or error that exists in an assertion or a control. Detection risk can be affected by factors such as the nature, timing, and extent of the audit procedures, the quality and sufficiency of the audit evidence, and the auditor's professional judgment and competence. Detection risk can be reduced by applying appropriate audit techniques, such as sampling, testing, observation, inquiry, and analysis. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 10
- (Topic 3)
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

Answer: B

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. References:
? CISA Review Manual, 27th Edition, page 1111
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 15
- (Topic 3)
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.

Answer: C

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. References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA], [Business Case- ISACA], [Tender - ISACA], [Procurement Management - ISACA]

NEW QUESTION 18
- (Topic 3)
An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in- house. Which of the following findings should be the IS auditor's GREATEST concern?

A. The cost of outsourcing is lower than in-house development.
B. The vendor development team is located overseas.
C. A training plan for business users has not been developed.
D. The data model is not clearly documented.

Answer: D

Explanation:
The finding that should be the IS auditor's greatest concern is that the data model is not clearly documented. A data model is a representation of the structure, relationships, and constraints of the data used by an application. It is a vital component of the software development process, as it helps to ensure the accuracy, consistency, and quality of the data1. A clear and comprehensive documentation of the data model is essential for the maintenance and support of the application, as it facilitates the understanding, modification, and troubleshooting of the data and the application logic2.
If the organization plans to bring the support and future maintenance of the application back in-house, it will need to have access to the data model documentation from the vendor. Without it, the organization may face difficulties in transferring the knowledge and skills from the vendor to the in-house team, as well as in adapting and enhancing the application to meet changing business needs and requirements3. The lack of data model documentation may also increase the risk of errors, inconsistencies, and inefficiencies in the data and the application performance2.

The other findings are not as concerning as the lack of data model documentation, because they do not directly affect the quality and maintainability of the application. The cost of outsourcing is lower than in-house development is a benefit rather than a risk for the organization, as it implies that outsourcing has helped to save time and money for the organization4. The vendor development team is located overseas is a common practice in outsourcing, and it does not necessarily imply a lower quality or a higher risk of the application. However, it may pose some challenges in terms of communication, coordination, and cultural differences, which can be managed by establishing clear expectations, roles, and responsibilities, as well as using effective tools and methods for communication and collaboration5. A training plan for business users has not been developed is a gap that should be addressed by the organization before deploying the application, as it may affect the user acceptance and satisfaction of the application. However, it does not directly impact the quality or maintainability of the application itself. References:
? What is Data Modeling? Definition & Types | Informatica1
? Data Modeling Best Practices: Documentation | erwin2
? Data Model Documentation - an overview | ScienceDirect Topics3
? Outsourcing App Development Pros and Cons – Droids On Roids4
? 8 Risks of Software Development Outsourcing & Their Solutions - Acropolium5
? Software Training Plan: How to Create One for Your Business - Elinext

NEW QUESTION 19
- (Topic 3)
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

Answer: A

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.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.6

NEW QUESTION 24
- (Topic 3)
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.

Answer: C

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. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 29
- (Topic 3)
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

Answer: B

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.
References:
? ISACA, CISA Review Manual, 27th Edition, 2020, page 247
? Data Classification: What It Is and How to Implement It

NEW QUESTION 34
- (Topic 2)
Which of the following is the MOST important reason to classify a disaster recovery plan (DRP) as confidential?

A. Ensure compliance with the data classification policy.
B. Protect the plan from unauthorized alteration.
C. Comply with business continuity best practice.
D. Reduce the risk of data leakage that could lead to an attack.

Answer: D

Explanation:
The most important reason to classify a disaster recovery plan (DRP) as confidential is to reduce the risk of data leakage that could lead to an attack. A DRP contains sensitive information about the organization's IT infrastructure, systems, processes, and procedures for recovering from a disaster. If this information falls into the wrong hands, it could be exploited by malicious actors to launch targeted attacks, sabotage recovery efforts, or extort ransom. Therefore, a DRP should be protected from unauthorized access, disclosure, modification, or destruction.
The other options are not as important as reducing the risk of data leakage that could lead to an attack:
? Ensuring compliance with the data classification policy is a good practice, but it is not a sufficient reason to classify a DRP as confidential. The data classification policy should reflect the level of risk and impact associated with each type of data, and a DRP should be classified as confidential based on its potential harm if compromised.
? Protecting the plan from unauthorized alteration is a valid concern, but it is not a primary reason to classify a DRP as confidential. A DRP should be protected from unauthorized alteration by implementing access controls, audit trails, version control, and change management processes. Classifying a DRP as confidential may deter some unauthorized alterations, but it does not prevent them.
? Complying with business continuity best practice is a desirable goal, but it is not a compelling reason to classify a DRP as confidential. Business continuity best practice may recommend classifying a DRP as confidential, but it does not mandate it. The decision to classify a DRP as confidential should be based on a risk assessment and a cost-benefit analysis.

NEW QUESTION 35
- (Topic 2)
Due to a recent business divestiture, an organization has limited IT resources to deliver critical projects Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

A. Human resources (HR) sourcing strategy
B. Records of actual time spent on projects
C. Peer organization staffing benchmarks
D. Budgeted forecast for the next financial year

Answer: B

Explanation:
The best source of information for IT management to estimate resource requirements for future projects is the records of actual time spent on projects. This data can provide a realistic and reliable basis for forecasting future resource needs based on historical trends and patterns. The records of actual time spent on projects can also help IT management to identify any gaps or inefficiencies in resource allocation and utilization. The human resources (HR) sourcing strategy is not a good source of information for estimating resource requirements for future projects, as it may not reflect the actual demand and availability of IT resources. The peer organization staffing benchmarks are not a good source of information for estimating resource requirements for future projects, as they may not account for the specific characteristics and needs of each organization. The budgeted forecast for the next financial year is not a good source of information for estimating resource requirements for future projects, as it may not be based on accurate or realistic assumptions. References:
? CISA Review Manual, 27th Edition, pages 465-4661
? CISA Review Questions, Answers & Explanations Database, Question ID: 263

NEW QUESTION 37
- (Topic 2)
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 web server.
B. the demilitarized zone (DMZ).
C. the organization's network.
D. the Internet

Answer: D

Explanation:
The best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet. An IDS is a device or software that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. By placing an IDS between the firewall and the Internet, the IS auditor can enhance the security of the network perimeter and detect any attack attempts that the firewall was unable to recognize.
The other options are not as effective as placing an IDS between the firewall and the Internet:
? Placing an IDS between the firewall and the organization's web server would not
protect the web server from external attacks that bypass the firewall. The web server should be placed in a demilitarized zone (DMZ), which is a separate network segment that isolates public-facing servers from the internal network.
? Placing an IDS between the firewall and the demilitarized zone (DMZ) would not protect the DMZ from external attacks that bypass the firewall. The DMZ should be protected by two firewalls, one facing the Internet and one facing the internal network, with an IDS monitoring both sides of each firewall.
? Placing an IDS between the firewall and the organization's network would not protect the organization's network from external attacks that bypass the firewall. The organization's network should be protected by a firewall that blocks unauthorized traffic from entering or leaving the network, with an IDS monitoring both sides of the firewall.

NEW QUESTION 41
- (Topic 2)
An organization has assigned two now IS auditors to audit a now system implementation. One of the auditors has an IT-related degree, and one has a business

degree. Which ol the following is MOST important to meet the IS audit standard for proficiency?

A. The standard is met as long as one member has a globally recognized audit certification.
B. Technical co-sourcing must be used to help the new staff.
C. Team member assignments must be based on individual competencies.
D. The standard is met as long as a supervisor reviews the new auditors' work.

Answer: C

Explanation:
Team member assignments based on individual competencies is the most important factor to meet the IS audit standard for proficiency. Proficiency is the ability to apply knowledge, skills and experience to perform audit tasks effectively and efficiently. The IS audit standard for proficiency requires that IS auditors must possess the knowledge, skills and discipline to perform audit tasks in accordance with applicable standards, guidelines and procedures. Team member assignments based on individual competencies is a way to ensure that each IS auditor is assigned to audit tasks that match their level of proficiency, and that the audit team as a whole has sufficient and appropriate proficiency to conduct the audit. The other options are not as important as option C, as they do not ensure that the IS auditors have the required proficiency to perform audit tasks. Having a globally recognized audit certification is a way to demonstrate proficiency in IS auditing, but it does not guarantee that the IS auditor has the specific knowledge, skills and experience needed for a particular audit task or system. Technical co-sourcing is a way to supplement the proficiency of the IS audit team by hiring external experts or consultants to perform certain audit tasks or functions, but it does not replace the need for internal IS auditors to have adequate proficiency. Having a supervisor review the new auditors' work is a way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

NEW QUESTION 45
- (Topic 2)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

A. The policy includes a strong risk-based approach.
B. The retention period allows for review during the year-end audit.
C. The retention period complies with data owner responsibilities.
D. The total transaction amount has no impact on financial reporting

Answer: C

Explanation:
The most important factor for the organization to ensure when reducing the retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for defining the retention and disposal requirements for the data under their custody, based on business, legal, regulatory, and contractual obligations. The policy should reflect the data owner's decisions and obtain their approval. The policy should also include a risk-based approach, but this is not as important as complying with data owner responsibilities. The retention period should allow for review during the year-end audit, but this may not be necessary for low-value transactions that have minimal impact on financial reporting. The total transaction amount may have some impact on financial reporting, but this is not a direct consequence of reducing the retention period. References:
? CISA Review Manual, 27th Edition, pages 414-4151
? CISA Review Questions, Answers & Explanations Database, Question ID: 255

NEW QUESTION 49
- (Topic 2)
Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

A. Ensure that the facts presented in the report are correct
B. Communicate the recommendations lo senior management
C. Specify implementation dates for the recommendations.
D. Request input in determining corrective action.

Answer: A

Explanation:
Ensuring that the facts presented in the report are correct is the most important thing for an IS auditor to do during an exit meeting with an auditee. An IS auditor should confirm that the audit findings and observations are accurate, complete, and supported by sufficient evidence, as well as that the auditee understands and agrees with them. This will help to avoid any misunderstandings or disputes later on, as well as to enhance the credibility and quality of the audit report. The other options are less important things for an IS auditor to do during an exit meeting, as they may involve communicating the recommendations to senior management, specifying implementation dates for the recommendations, or requesting input in determining corrective action. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21
? CISA Review Questions, Answers & Explanations Database, Question ID 222

NEW QUESTION 53
- (Topic 2)
Which of the following is the BEST audit procedure to determine whether a firewall is configured in compliance with the organization's security policy?

A. Reviewing the parameter settings
B. Reviewing the system log
C. Interviewing the firewall administrator
D. Reviewing the actual procedures

Answer: A

Explanation:
The best audit procedure to determine whether a firewall is configured in compliance with the organization's security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter settings of a firewall, an IS auditor can verify whether they match with the organization's security policy, which is a document that outlines the security objectives,

requirements, and guidelines for an organization's information systems and resources. Reviewing the system log is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a system log records events or activities that occur on a firewall, such as connections, requests, responses, errors, alerts, etc., and may not indicate whether they comply with the organization's security policy. Interviewing the firewall administrator is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a firewall administrator may not provide accurate or reliable information about the firewall configuration, and may have conflicts of interest or ulterior motives. Reviewing the actual procedures is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as actual procedures describe how a firewall is configured and maintained, such as installation, testing, updating, etc., and may not reflect whether they comply with the organization's security policy.

NEW QUESTION 55
- (Topic 2)
An IS auditor Is reviewing a recent security incident and is seeking information about me approval of a recent modification to a database system's security settings Where would the auditor MOST likely find this information?

A. System event correlation report
B. Database log
C. Change log
D. Security incident and event management (SIEM) report

Answer: C

Explanation:
A change log is a record of all changes made to a system or application, including the date, time, description, and approval of each change. A change log can help an IS auditor to trace the source and authorization of a modification to a system's security settings. A system event correlation report is a tool that analyzes data from multiple sources to identify patterns and anomalies that indicate potential security incidents. A database log is a record of all transactions and activities performed on a database, such as queries, updates, and backups. A security incident and event management (SIEM) report is a tool that collects, analyzes, and reports on data from various sources to detect and respond to security incidents.

NEW QUESTION 57
- (Topic 2)
While auditing a small organization's data classification processes and procedures, an IS auditor noticed that data is often classified at the incorrect level. What is the MOST effective way for the organization to improve this situation?

A. Use automatic document classification based on content.
B. Have IT security staff conduct targeted training for data owners.
C. Publish the data classification policy on the corporate web portal.
D. Conduct awareness presentations and seminars for information classification policies.

Answer: B

Explanation:
This is the most effective way for the organization to improve its data classification processes and procedures, because data owners are the ones who are responsible for assigning the appropriate level of classification to the data they create, collect, or manage. Data owners should be aware of the data classification policy, the criteria for each level of classification, and the implications of misclassification. IT security staff can provide tailored training for data owners based on their roles, functions, and types of data they handle.
The other options are not as effective as having IT security staff conduct targeted training for data owners:
? Use automatic document classification based on content. This is a possible option, but it may not be feasible or accurate for a small organization. Automatic document classification is a process that uses artificial intelligence or machine learning to analyze the content of a document and assign a class label based on predefined rules or models. However, this process may require a lot of resources, expertise, and maintenance, and it may not capture all the nuances and context of the data. The IS auditor should also verify the reliability and validity of the automatic document classification system.
? Publish the data classification policy on the corporate web portal. This is a good practice, but it is not enough to improve the data classification situation. Publishing the data classification policy on the corporate web portal can increase the visibility and accessibility of the policy, but it does not ensure that data owners will read, understand, and follow it. The IS auditor should also monitor and enforce the compliance with the policy.
? Conduct awareness presentations and seminars for information classification policies. This is a useful measure, but it is not the most effective one. Conducting awareness presentations and seminars can raise the general awareness and knowledge of information classification policies among all employees, but it may not address the specific needs and challenges of data owners. The IS auditor should also provide more in-depth and practical training for data owners.

NEW QUESTION 58
- (Topic 2)
Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

A. The job scheduler application has not been designed to display pop-up error messages.
B. Access to the job scheduler application has not been restricted to a maximum of two staff members
C. Operations shift turnover logs are not utilized to coordinate and control the processing environment
D. Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor

Answer: D

Explanation:
Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor. This is a serious control weakness that could compromise the integrity, availability, and security of the IT operations. An IS auditor should be concerned about the lack of oversight and accountability for such changes, which could result in unauthorized, erroneous, or malicious modifications that affect the processing environment. The other options are less critical issues that may not have a significant impact on the IT operations. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.11
? CISA Review Questions, Answers & Explanations Database, Question ID 202

NEW QUESTION 63
- (Topic 2)
A project team has decided to switch to an agile approach to develop a replacement for an existing business application. Which of the following should an IS

auditor do FIRST to ensure the effectiveness of the protect audit?

A. Compare the agile process with previous methodology.
B. Identify and assess existing agile process control
C. Understand the specific agile methodology that will be followed.
D. Interview business process owners to compile a list of business requirements

Answer: C

Explanation:
Understanding the specific agile methodology that will be followed is the first step that an IS auditor should do to ensure the effectiveness of the project audit. An IS auditor should familiarize themselves with the agile approach, principles, practices, and tools that will be used by the project team, as well as the roles and responsibilities of the project stakeholders. This will help the IS auditor to identify and assess the relevant risks and controls for the project audit. The other options are not the first steps that an IS auditor should do, but rather possible subsequent actions that may depend on the specific agile methodology. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.21
? CISA Review Questions, Answers & Explanations Database, Question ID 211

NEW QUESTION 68
- (Topic 2)
In order to be useful, a key performance indicator (KPI) MUST

A. be approved by management.
B. be measurable in percentages.
C. be changed frequently to reflect organizational strategy.
D. have a target value.

Answer: D

Explanation:
A key performance indicator (KPI) is a quantifiable measure of performance over time for a specific objective1. KPIs help organizations and teams track their progress and achievements towards their strategic goals. To be useful, a KPI must have a target value, which is the desired level of performance or outcome that the organization or team aims to achieve. A target value provides a clear direction and a benchmark for measuring success or failure. Without a target value, a KPI is meaningless, as it does not indicate whether the performance is good or bad, or how far or close the organization or team is from reaching their objective.

NEW QUESTION 72
- (Topic 2)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

A. Obtain error codes indicating failed data feeds.
B. Purchase data cleansing tools from a reputable vendor.
C. Appoint data quality champions across the organization.
D. Implement business rules to reject invalid data.

Answer: D

Explanation:
The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical statements that define the data quality requirements and standards for the organization. By implementing business rules, the organization can ensure that only data that meets the predefined criteria is accepted into the enterprise data warehouse. Obtaining error codes indicating failed data feeds, purchasing data cleansing tools from a reputable vendor, and appointing data quality champions across the organization are useful measures to improve data quality, but they do not prevent accepting bad data in the first place. References:
ISACA Journal Article: Data Quality Management

NEW QUESTION 75
- (Topic 2)
During a follow-up audit, it was found that a complex security vulnerability of low risk was not resolved within the agreed-upon timeframe. IT has stated that the system with the identified vulnerability is being replaced and is expected to be fully functional in two months Which of the following is the BEST course of action?

A. Require documentation that the finding will be addressed within the new system
B. Schedule a meeting to discuss the issue with senior management
C. Perform an ad hoc audit to determine if the vulnerability has been exploited
D. Recommend the finding be resolved prior to implementing the new system

Answer: A

Explanation:
Requiring documentation that the finding will be addressed within the new system is the best course of action for a follow-up audit. An IS auditor should obtain evidence that the complex security vulnerability of low risk will be resolved in the new system and that there is a reasonable timeline for its implementation. The other options are not appropriate courses of action, as they may be too costly, time-consuming, or impractical for a low-risk finding. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
? CISA Review Questions, Answers & Explanations Database, Question ID 209

NEW QUESTION 78
- (Topic 2)
The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

A. the access control system's log settings.
B. how the latest system changes were implemented.

C. the access control system's configuration.
D. the access rights that have been granted.

Answer: D

Explanation:
The best way to determine whether programmers have permission to alter data in the production environment is by reviewing the access rights that have been granted. Access rights are permissions or privileges that define what actions or operations a user can perform on an information system or resource. By reviewing the access rights that have been granted to programmers, an IS auditor can verify whether they have been authorized to modify data in the production environment, which is where live data and applications are stored and executed. The access control system's log settings are parameters that define what events or activities are recorded by the access control system, which is a system that enforces the access rights and policies of an information system or resource. The access control system's log settings are not the best way to determine whether programmers have permission to alter data in the production environment, as they do not indicate what permissions or privileges have been granted to programmers. How the latest system changes were implemented is a process that describes how software updates or modifications are deployed to the production environment. How the latest system changes were implemented is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers. The access control system's configuration is a set of rules or parameters that define how the access control system operates and functions. The access control system's configuration is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers.

NEW QUESTION 82
- (Topic 2)
In an online application which of the following would provide the MOST information about the transaction audit trail?

A. File layouts
B. Data architecture
C. System/process flowchart
D. Source code documentation

Answer: C

Explanation:
The most information about the transaction audit trail in an online application can be obtained by reviewing the system/process flowchart. A system/process flowchart is a diagram that illustrates the sequence of steps, activities, or events that occur within or affect a system or process. A system/process flowchart can provide the most information about the transaction audit trail in an online application, by showing how transactions are initiated, processed, recorded, and completed, and identifying the inputs, outputs, controls, and dependencies involved in each transaction. File layouts are specifications that define how data are structured or organized on a file or database. File layouts can provide some information about the transaction audit trail in an online application, by showing what data elements are stored or retrieved for each transaction, but they do not provide information about how transactions are executed or tracked. Data architecture is a framework that defines how data are collected, stored, managed, and used within an organization or system. Data architecture can provide some information about the transaction audit trail in an online application, by showing what data sources, models, standards, and policies are used for each transaction, but they do not provide information about how transactions are performed or monitored. Source code documentation is a description or explanation of the source code of a software program or application. Source code documentation can provide some information about the transaction audit trail in an online application, by showing what logic, algorithms, or functions are used for each transaction, but they do not provide information about how transactions are handled or audited.

NEW QUESTION 84
- (Topic 2)
Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

A. Legal and compliance requirements
B. Customer agreements
C. Data classification
D. Organizational policies and procedures

Answer: D

Explanation:
The organizational policies and procedures are the first source of guidance for an IS auditor when planning a customer data privacy audit. They provide the framework and objectives for ensuring compliance with legal and regulatory requirements, customer agreements and data classification. The IS auditor should review them first to understand the scope, roles and responsibilities, standards and controls related to customer data privacy in the organization. The other options are also important, but they are secondary sources of information that should be reviewed after the organizational policies and procedures. References: CISA Review Manual (Digital Version) 1, Chapter 2: Governance and Management of Information Technology, Section 2.5: Privacy Principles and Policies.

NEW QUESTION 88
- (Topic 2)
An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

A. Users are not required to sign updated acceptable use agreements.
B. Users have not been trained on the new system.
C. The business continuity plan (BCP) was not updated.
D. Mobile devices are not encrypted.

Answer: C

Explanation:
This should be the IS auditor's greatest concern, because it means that the organization has not considered the potential impact of the cloud document storage solution on its ability to continue its operations in the event of a disruption or disaster. A BCP is a document that outlines the procedures and actions to be taken in order to maintain or resume critical business functions during and after a crisis. A BCP should be updated whenever there is a significant change in the organization's IT infrastructure, systems, processes, or dependencies, such as implementing a cloud document storage solution. The IS auditor should verify that the BCP reflects the current state of the organization's IT environment, and that it addresses the risks, challenges, and opportunities associated with the cloud

document storage solution.
The other options are not as concerning as the BCP not being updated:
? Users are not required to sign updated acceptable use agreements. This is a minor concern, but it does not pose a major threat to the organization's business continuity. Acceptable use agreements are documents that define the rules and guidelines for using IT resources, such as the cloud document storage solution. Users should sign updated acceptable use agreements to acknowledge their responsibilities and obligations, and to comply with the organization's policies and standards. However, this does not affect the organization's ability to continue its operations in a crisis.
? Users have not been trained on the new system. This is a moderate concern, but it does not jeopardize the organization's business continuity. Training users on the new system is important to ensure that they can use it effectively and efficiently, and to avoid errors or misuse that could compromise the security or performance of the system. However, this does not prevent the organization from accessing or restoring its data in a crisis.
? Mobile devices are not encrypted. This is a serious concern, but it does not directly impact the organization's business continuity. Encrypting mobile devices is a security measure that protects the data stored on them from unauthorized access or disclosure in case of loss or theft. However, this does not affect the availability or integrity of the data stored in the cloud document storage solution, which should have its own encryption mechanisms.

NEW QUESTION 89
- (Topic 2)
An IS auditor notes that IT and the business have different opinions on the availability of their application servers. Which of the following should the IS auditor review FIRST in order to understand the problem?

A. The exact definition of the service levels and their measurement
B. The alerting and measurement process on the application servers
C. The actual availability of the servers as part of a substantive test
D. The regular performance-reporting documentation

Answer: A

Explanation:
The exact definition of the service levels and their measurement is the first thing that the IS auditor should review in order to understand the problem of different opinions on the availability of their application servers. Service levels are the agreed-upon standards or targets for delivering IT services, such as availability, reliability, performance, and security. Service level measurement is the process of collecting, analyzing, and reporting data related to the achievement of service levels. By reviewing the exact definition of the service levels and their measurement, the IS auditor can identify any gaps, inconsistencies, or ambiguities that may cause confusion or disagreement among IT and the business. The other options are not as important as reviewing the exact definition of the service levels and their measurement, as they do not address the root cause of the problem. References: CISA Review Manual, 27th Edition, page 372

NEW QUESTION 90
- (Topic 2)
Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor's BEST recommendation for a compensating control?

A. Require written authorization for all payment transactions
B. Restrict payment authorization to senior staff members.
C. Reconcile payment transactions with invoices.
D. Review payment transaction history

Answer: A

Explanation:
Requiring written authorization for all payment transactions is the IS auditor's best recommendation for a compensating control in an environment where segregation of duties (SoD) cannot be enforced in an accounts payable system. SoD is a principle that requires different individuals or functions to perform different tasks or roles in a business process, such as initiating, approving, recording and reconciling transactions. SoD reduces the risk of errors, fraud and misuse of resources by preventing any single person or function from having excessive or conflicting authority or responsibility. A compensating control is a control that mitigates or reduces the risk associated with the absence or weakness of another control. Requiring written authorization for all payment transactions is a compensating control that provides an independent verification and approval of each transaction before it is processed by the accounts payable system. This control can help to detect and prevent unauthorized, duplicate or erroneous payments, and to ensure compliance with policies and procedures. The other options are not as effective as option A, as they do not provide an independent verification or approval of payment transactions. Restricting payment authorization to senior staff members is a control that limits the number of people who can authorize payments, but it does not prevent them from initiating or processing payments themselves, which could violate SoD. Reconciling payment transactions with invoices is a control that verifies that the payments match the invoices, but it does not prevent unauthorized, duplicate or erroneous payments from being processed by the accounts payable system. Reviewing payment transaction history is a control that monitors and analyzes the payment transactions after they have been processed by the accounts payable system, but it does not prevent unauthorized, duplicate
or erroneous payments from occurring in the first place. References: CISA Review Manual
(Digital Version) , Chapter 5: Protection of Information Assets, Section 5.2: Logical Access.

NEW QUESTION 93
- (Topic 2)
Which of the following would BEST manage the risk of changes in requirements after the analysis phase of a business application development project?

A. Expected deliverables meeting project deadlines
B. Sign-off from the IT team
C. Ongoing participation by relevant stakeholders
D. Quality assurance (OA) review

Answer: B

NEW QUESTION 94
- (Topic 2)
A new regulation in one country of a global organization has recently prohibited cross- border transfer of personal data. An IS auditor has been asked to determine the organization's level of exposure In the affected country. Which of the following would be MOST helpful in making this assessment?

A. Developing an inventory of all business entities that exchange personal data with the affected jurisdiction

B. Identifying data security threats in the affected jurisdiction
C. Reviewing data classification procedures associated with the affected jurisdiction
D. Identifying business processes associated with personal data exchange with the affected jurisdiction

Answer: D

Explanation:
Identifying business processes associated with personal data exchange with the affected jurisdiction is the most helpful activity in making an assessment of the organization's level of exposure in the affected country. An IS auditor should understand how the organization's business operations and functions rely on or involve the cross- border transfer of personal data, as well as the potential impacts and risks of the new regulation on the business continuity and compliance. The other options are less helpful activities that may provide additional information or context for the assessment, but not its
primary focus. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
? CISA Review Questions, Answers & Explanations Database, Question ID 221

NEW QUESTION 98
- (Topic 2)
During an audit of a multinational bank's disposal process, an IS auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

A. Backup media are not reviewed before disposal.
B. Degaussing is used instead of physical shredding.
C. Backup media are disposed before the end of the retention period
D. Hardware is not destroyed by a certified vendor.

Answer: C

Explanation:
During an audit of a multinational bank's disposal process, an IS auditor should be most concerned about backup media being disposed before the end of the retention period. This is because backup media contain sensitive and critical data that may be required for business continuity, legal compliance, or forensic purposes. Disposing backup media prematurely may result in data loss, unavailability, or corruption, which may have severe consequences for the bank's reputation, operations, and security. Backup media not being reviewed before disposal, degaussing being used instead of physical shredding, and hardware not being destroyed by a certified vendor are also findings that may pose some risks to the bank's disposal process, but they are not as critical as backup media being disposed before the end of the retention period. References: ISACA CISA Review Manual 27th Edition, page 302.

NEW QUESTION 103
- (Topic 2)
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control sell-assessment (CSA)?

A. Implementing the remediation plan
B. Partially completing the CSA
C. Developing the remediation plan
D. Developing the CSA questionnaire

Answer: D

Explanation:
Developing the CSA questionnaire is an activity that would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA). An IS auditor can design and provide a CSA questionnaire to help the business units or process owners to evaluate their own controls and identify any issues or improvement opportunities. This will enable an IS auditor to support and guide the CSA process without compromising their objectivity or independence. The other options are activities that would impair an IS auditor's independence while facilitating a CSA, as they involve implementing, completing, or developing remediation actions for control issues. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.41
? CISA Review Questions, Answers & Explanations Database, Question ID 215

NEW QUESTION 108
- (Topic 2)
Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simu-lation test administered for staff members?

A. Staff members who failed the test did not receive follow-up education
B. Test results were not communicated to staff members.
C. Staff members were not notified about the test beforehand.
D. Security awareness training was not provided prior to the test.

Answer: A

Explanation:
The IS auditor should be most concerned about the lack of follow-up education for staff members who failed the phishing simulation test. Phishing simulation tests are designed to assess the level of awareness and susceptibility of staff members to phishing attacks, and to provide feedback and training to improve their security behavior. If staff members who failed the test do not receive follow-up education, they will not learn from their mistakes and may continue to fall victim to real phishing attacks, which could compromise the security of the organization.
The other options are less concerning for the IS auditor:
? Test results were not communicated to staff members. This is not ideal, as staff members should receive feedback on their performance and learn from the test results. However, this does not necessarily mean that they did not receive any training or education on how to avoid phishing attacks.
? Staff members were not notified about the test beforehand. This is a common practice for phishing simulation tests, as it mimics the real-world scenario where staff members do not know when they will receive a phishing email. The purpose of the test is to measure their spontaneous reaction and awareness, not their preparedness or compliance.
? Security awareness training was not provided prior to the test. This is not a major concern, as the test can serve as a baseline measurement of the current level of awareness and susceptibility of staff members, and as a starting point for providing tailored training and education based on the test results.

NEW QUESTION 113
- (Topic 2)
Which of the following is an example of a preventative control in an accounts payable system?

A. The system only allows payments to vendors who are included In the system's master vendor list.
B. Backups of the system and its data are performed on a nightly basis and tested periodically.
C. The system produces daily payment summary reports that staff use to compare against invoice totals.
D. Policies and procedures are clearly communicated to all members of the accounts payable department

Answer: A

Explanation:
The system only allows payments to vendors who are included in the system's master vendor list is an example of a preventative control in an accounts payable system. A preventative control is a control that aims to prevent errors or irregularities from occurring in the first place. By restricting payments to vendors who are authorized and verified in the master vendor list, the system prevents unauthorized or fraudulent payments from being made. The other options are examples of other types of controls, such as backup (recovery), reconciliation (detective), and communication (directive) controls.
References: CISA Review Manual, 27th Edition, page 223

NEW QUESTION 116
- (Topic 2)
Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

A. Service management standards are not followed.
B. Expected time to resolve incidents is not specified.
C. Metrics are not reported to senior management.
D. Prioritization criteria are not defined.

Answer: D

Explanation:
he design of an incident management process should include prioritization criteria to ensure that incidents are handled according to their impact and urgency. Without prioritization criteria, the organization may not be able to allocate resources effectively and respond to incidents in a timely manner. Expected time to resolve incidents, service management standards, and metrics reporting are important aspects of incident management, but they are not as critical as prioritization criteria for the design of the process. References: ISACA Journal Article: Incident Management: A Practical Approach

NEW QUESTION 118
- (Topic 2)
The IS auditor has recommended that management test a new system before using it in production mode. The BEST approach for management in developing a test plan is to use processing parameters that are:

A. randomly selected by a test generator.
B. provided by the vendor of the application.
C. randomly selected by the user.
D. simulated by production entities and customers.

Answer: D

Explanation:
The best approach for management in developing a test plan is to use processing parameters that are simulated by production entities and customers. This is because using realistic data and scenarios can help to evaluate the functionality, performance, reliability, and security of the new system under actual operating conditions and expectations. Using processing parameters that are randomly selected by a test generator, provided by the vendor of the application, or randomly selected by the user may not be sufficient or representative of the production environment and may not reveal all the potential issues or defects of the new system. References: [ISACA CISA Review Manual 27th Edition], page 266.

NEW QUESTION 123
- (Topic 2)
During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

A. reflect current practices.
B. include new systems and corresponding process changes.
C. incorporate changes to relevant laws.
D. be subject to adequate quality assurance (QA).

Answer: A

Explanation:
The greatest concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated is that policies and procedures might not reflect current practices. Policies are documents that define the goals, objectives, and guidelines for an organization's information systems and resources. Procedures are documents that describe the steps, tasks, or activities for implementing or executing policies. Policies and procedures should be regularly reviewed and updated to ensure that they are relevant, accurate, consistent, and effective for the organization's information systems and resources. Policies and procedures that are not regularly reviewed and updated might not reflect current practices, as they might be outdated, obsolete, or incompatible with the current state or needs of the organization's information systems and resources. This can cause confusion, inconsistency, inefficiency, or noncompliance among users or stakeholders who rely on policies and procedures for guidance or direction. Policies and procedures might not include new systems and corresponding process changes is a possible concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated, but it is not the greatest one. Policies and procedures might not include new systems and corresponding process changes, as they might be unaware of or unresponsive to the introduction or modification of information systems or resources within the organization. This can cause gaps, overlaps, or conflicts among policies and procedures that affect different information systems or resources.

NEW QUESTION 125
- (Topic 2)
Which of the following would MOST effectively ensure the integrity of data transmitted over a network?

A. Message encryption
B. Certificate authority (CA)
C. Steganography
D. Message digest

Answer: D

Explanation:
The most effective way to ensure the integrity of data transmitted over a network is to use a message digest. A message digest is a cryptographic function that generates a unique and fixed-length value (also known as a hash or checksum) from any input data. The message digest can be used to verify that the data has not been altered or corrupted during transmission by comparing it with the message digest generated at the destination. Message encryption is a method of protecting the confidentiality of data transmitted over a network by transforming it into an unreadable format using a secret key. Message encryption does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Certificate authority (CA) is an entity that issues and manages digital certificates that bind public keys to identities. CA does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Steganography is a technique of hiding data within other data, such as images or audio files. Steganography does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. References:
? CISA Review Manual, 27th Edition, pages 383-3841
? CISA Review Questions, Answers & Explanations Database, Question ID: 258

NEW QUESTION 126
- (Topic 2)
Which of the following Is the BEST way to ensure payment transaction data is restricted to the appropriate users?

A. Implementing two-factor authentication
B. Restricting access to transactions using network security software
C. implementing role-based access at the application level
D. Using a single menu tor sensitive application transactions

Answer: C

Explanation:
The best way to ensure payment transaction data is restricted to the appropriate users is implementing role-based access at the application level. Role-based access is a method of access control that assigns permissions or privileges to users based on their roles or functions within an organization or system. Role-based access can help ensure that payment transaction data is restricted to the appropriate users, by allowing only authorized users who have a legitimate need or purpose to access or use the payment transaction data, and preventing unauthorized or unnecessary access or use by other users. Implementing two-factor authentication is a possible way to enhance the security and verification of user identities, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not define what permissions or privileges users have on the payment transaction data. Restricting access to transactions using network security software is a possible way to protect the network communication and transmission of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not specify what actions or operations users can perform on the payment transaction data. Using a single menu for sensitive application transactions is a possible way to simplify the user interface and navigation of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not limit what users can access or use the payment transaction data.

NEW QUESTION 129
- (Topic 2)
Which of the following are BEST suited for continuous auditing?

A. Low-value transactions
B. Real-lime transactions
C. Irregular transactions
D. Manual transactions

Answer: B

Explanation:
Continuous auditing is a method of performing audit-related activities on a real-time or near real-time basis. Continuous auditing is best suited for real-time transactions, such as online banking, e-commerce, or electronic funds transfer, that require immediate verification and assurance. Low-value transactions are not necessarily suitable for continuous auditing, as they may not pose significant risks or require frequent monitoring. Irregular transactions are not suitable for continuous auditing, as they may not occur frequently or consistently enough to justify the use of continuous auditing techniques. Manual transactions are not suitable for continuous auditing, as they may not be captured or processed by automated systems that enable continuous auditing. References:
? CISA Review Manual, 27th Edition, pages 307-3081
? CISA Review Questions, Answers & Explanations Database, Question ID: 253

NEW QUESTION 133
- (Topic 2)
Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

A. Availability of IS audit resources
B. Remediation dates included in management responses
C. Peak activity periods for the business
D. Complexity of business processes identified in the audit

Answer: B

Explanation:
The most important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings is the remediation dates included

in management responses. The IS auditor should ensure that the follow-up activities are aligned with the agreed-upon action plans and deadlines that management has committed to in response to the audit findings. The follow-up activities should verify that management has implemented the corrective actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are less important factors for establishing timeframes for follow-up activities:
? Availability of IS audit resources. This is a practical factor that may affect the scheduling and execution of follow-up activities, but it should not override the priority and urgency of verifying management's corrective actions.
? Peak activity periods for the business. This is a factor that may affect the availability and cooperation of auditees during follow-up activities, but it should not delay or postpone the verification of management's corrective actions beyond reasonable limits.
? Complexity of business processes identified in the audit. This is a factor that may affect the scope and depth of follow-up activities, but it should not affect the timeframe for verifying management's corrective actions.

NEW QUESTION 137
- (Topic 2)
Which of the following concerns is BEST addressed by securing production source libraries?

A. Programs are not approved before production source libraries are updated.
B. Production source and object libraries may not be synchronized.
C. Changes are applied to the wrong version of production source libraries.
D. Unauthorized changes can be moved into production.

Answer: D

Explanation:
Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21
? CISA Review Questions, Answers & Explanations Database, Question ID 213

NEW QUESTION 141
- (Topic 2)
Which of the following is the PRIMARY role of the IS auditor m an organization's information classification process?

A. Securing information assets in accordance with the classification assigned
B. Validating that assets are protected according to assigned classification
C. Ensuring classification levels align with regulatory guidelines
D. Defining classification levels for information assets within the organization

Answer: B

Explanation:
Validating that assets are protected according to assigned classification is the primary role of the IS auditor in an organization's information classification process. An IS auditor should evaluate whether the information security controls are adequate and effective in safeguarding the information assets based on their classification levels. The other options are not the primary role of the IS auditor, but rather the responsibilities of the information owners, custodians, or security managers. References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 206

NEW QUESTION 142
- (Topic 2)
An IS audit learn is evaluating the documentation related to the most recent application user-access review performed by IT and business management It is determined that the user list was not system-generated. Which of the following should be the GREATEST concern?

A. Availability of the user list reviewed
B. Confidentiality of the user list reviewed
C. Source of the user list reviewed
D. Completeness of the user list reviewed

Answer: C

NEW QUESTION 144
- (Topic 2)
In an environment that automatically reports all program changes, which of the following is the MOST efficient way to detect unauthorized changes to production programs?

A. Reviewing the last compile date of production programs
B. Manually comparing code in production programs to controlled copies
C. Periodically running and reviewing test data against production programs
D. Verifying user management approval of modifications

Answer: A

Explanation:
Reviewing the last compile date of production programs is the most efficient way to detect unauthorized changes to production programs, as it can quickly identify any discrepancies between the expected and actual dates of program modification. The last compile date is a timestamp that indicates when a program was last compiled or translated from source code to executable code. Any changes to the source code would require a recompilation, which would update the last compile date. The IS auditor can compare the last compile date of production programs with the authorized change requests and reports to verify that only approved

changes were implemented. The other options are not as efficient as option A, as they are more time-consuming, labor-intensive or error-prone. Manually comparing code in production programs to controlled copies is a method of verifying that the code in production matches the code in a secure repository or library, but it requires access to both versions of code and a tool or technique to compare them line by line. Periodically running and reviewing test data against production programs is a method of verifying that the programs produce the expected outputs and results, but it requires designing, executing and evaluating test cases for each program. Verifying user management approval of modifications is a method of verifying that the changes to production programs were authorized and documented, but it does not ensure that the changes were implemented correctly or accurately. References: CISA Review Manual (Digital Version) , Chapter 4: Information Systems Operations and Business Resilience, Section 4.3: Change Management Practices.

NEW QUESTION 149
- (Topic 1)
Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

A. Identifying relevant roles for an enterprise IT governance framework
B. Making decisions regarding risk response and monitoring of residual risk
C. Verifying that legal, regulatory, and contractual requirements are being met
D. Providing independent and objective feedback to facilitate improvement of IT processes

Answer: D

Explanation:
The most important benefit of involving IS audit when implementing governance of enterprise IT is providing independent and objective feedback to facilitate improvement of IT processes. Governance of enterprise IT is the process of ensuring that IT supports the organization's strategy, goals, and objectives in an effective, efficient, ethical, and compliant manner. IS audit can provide value to governance of enterprise IT by assessing the alignment of IT with business needs, evaluating the performance and value delivery of IT, identifying risks and issues related to IT, recommending corrective actions and best practices, and monitoring the implementation and effectiveness of IT governance activities. IS audit can also provide assurance that IT governance processes are designed and operating in accordance with relevant standards, frameworks, laws, regulations, and contractual obligations. Identifying relevant roles for an enterprise IT governance framework is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help define and clarify the roles and responsibilities of various stakeholders involved in IT governance, such as board members, senior management, business units, IT function, external parties, etc. IS audit can also help ensure that these roles are aligned with the organization's strategy, goals, and objectives, and that they have adequate authority, accountability, communication, and reporting mechanisms. However, this benefit is more related to the design phase of IT governance implementation than to the ongoing monitoring and improvement phase. Making decisions regarding risk response and monitoring of residual risk is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help identify and assess the risks associated with IT activities and processes, such as
strategic risks, operational risks, compliance risks, security risks, etc. IS audit can also help evaluate the effectiveness of risk management practices and controls implemented by management to mitigate or reduce these risks. However, this benefit is more related to the assurance function of IS audit than to its advisory function. Verifying that legal, regulatory, and contractual requirements are being met is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help verify that IT activities and processes comply with applicable laws, regulations, and contractual obligations, such as data protection laws, privacy laws, cybersecurity laws, industry standards, service level agreements, etc. IS audit can also help identify and report any instances of noncompliance or violations that could result in legal or reputational consequences for the organization. However, this benefit is more related to the assurance function of IS audit than to its advisory function. References: ISACA CISA Review Manual 27th Edition, page 283

NEW QUESTION 152
- (Topic 1)
Which of the following is an audit reviewer's PRIMARY role with regard to evidence?

A. Ensuring unauthorized individuals do not tamper with evidence after it has been captured
B. Ensuring evidence is sufficient to support audit conclusions
C. Ensuring appropriate statistical sampling methods were used
D. Ensuring evidence is labeled to show it was obtained from an approved source

Answer: B

Explanation:
The primary role of an audit reviewer with regard to evidence is to ensure that evidence is sufficient to support audit conclusions. Evidence is the information obtained by the auditor to provide a reasonable basis for the audit opinion or findings. Evidence should be sufficient, reliable, relevant, and useful to support the audit objectives and criteria. The audit reviewer should evaluate the quality and quantity of evidence collected by the auditor and determine if it is adequate to draw valid conclusions and
recommendations. Ensuring unauthorized individuals do not tamper with evidence after it has been captured is a role of the auditor, not the audit reviewer. The auditor is responsible for safeguarding the evidence from loss, damage, or alteration during the audit process. The auditor should also document the source, date, and method of obtaining the evidence, as well as any limitations or restrictions on its use or disclosure. Ensuring appropriate statistical sampling methods were used is a role of the auditor, not the audit reviewer. The auditor is responsible for selecting an appropriate sampling method and technique that can provide sufficient evidence to achieve the audit objectives and criteria. The auditor should also document the sampling plan, population, sample size, selection method, evaluation method, and results. Ensuring evidence is labeled to show it was obtained from an approved source is a role of the auditor, not the audit reviewer. The auditor is responsible for labeling the evidence to indicate its origin, nature, and ownership. The auditor should also ensure that the evidence is obtained from reliable and credible sources that can be verified and corroborated. References: ISACA CISA Review Manual 27th Edition, page 295

NEW QUESTION 157
- (Topic 1)
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 Internet.
B. the demilitarized zone (DMZ).
C. the organization's web server.
D. the organization's network.

Answer: A

Explanation:
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 the Internet, as this would provide an additional layer of security and alert the organization of any malicious traffic that bypasses or penetrates the firewall. Placing an IDS between the firewall and the demilitarized zone (DMZ), the organization's web server, or the organization's network would not be as effective, as it would only monitor the traffic that has already passed through the firewall. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.3

NEW QUESTION 158
- (Topic 1)
The implementation of an IT governance framework requires that the board of directors of an organization:

A. Address technical IT issues.
B. Be informed of all IT initiatives.
C. Have an IT strategy committee.
D. Approve the IT strategy.

Answer: D

Explanation:
IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. The board of directors of an organization is ultimately accountable for IT governance and has the authority to approve the IT strategy. The board of directors does not need to address technical IT issues, be informed of all IT initiatives, or have an IT strategy committee, as these tasks can be delegated to other stakeholders or committees within the organization.

NEW QUESTION 163
- (Topic 1)
An organization has recently acquired and implemented intelligent-agent software for granting loans to customers. During the post-implementation review, which of the following is the MOST important procedure for the IS auditor to perform?

A. Review system and error logs to verify transaction accuracy.
B. Review input and output control reports to verify the accuracy of the system decisions.
C. Review signed approvals to ensure responsibilities for decisions of the system are welldefined.
D. Review system documentation to ensure completeness.

Answer: B

Explanation:
Reviewing input and output control reports to verify the accuracy of the system decisions is the most important procedure for the IS auditor to perform during the post-implementation review of intelligent-agent software for granting loans to customers, because it can help identify any errors or anomalies in the system logic or data that may affect the quality and reliability of the system outcomes. Reviewing system and error logs, signed approvals, and system documentation are also important procedures, but they are not as critical as verifying the accuracy of the system decisions. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21

NEW QUESTION 165
- (Topic 1)
Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).
B. Determine reporting requirements for vulnerabilities.
C. Define the testing scope.
D. Obtain management consent for the testing.

Answer: D

Explanation:
The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against the organization's systems and networks, which may have legal, ethical, and operational implications. Without proper authorization from management, a penetration test may violate laws, policies, contracts, or service level agreements. Management consent also helps define the objectives, scope, and boundaries of the test, as well as the roles and responsibilities of the testers and the stakeholders. Obtaining management consent for the testing also demonstrates due care and due diligence on the part of the testers and the organization.
Executing nondisclosure agreements (NDAs), determining reporting requirements for vulnerabilities, and defining the testing scope are important steps when planning a penetration test, but they are not the first step. These steps should be done after obtaining management consent for the testing, as they depend on the approval and involvement of management and other parties.

NEW QUESTION 166
- (Topic 1)
During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

A. allocation of resources during an emergency.
B. frequency of system testing.
C. differences in IS policies and procedures.
D. maintenance of hardware and software compatibility.

Answer: A

Explanation:
During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be most concerned with the allocation of resources during an emergency. A reciprocal disaster recovery agreement is an arrangement by which one organization agrees to use another's resources in the event of a business continuity event or incident. The IS auditor would need to ensure that both parties have clearly defined their roles and responsibilities, their resource requirements, their priority levels, their communication channels, and their escalation procedures in case of a disaster. The IS auditor would also need to verify that both parties have tested their agreement and have updated it regularly to reflect any changes in their business environments. The frequency of system testing is

not as critical as the allocation of resources during an emergency, because system testing can be performed periodically or on demand, while resource allocation is a dynamic and complex process that requires careful planning and coordination. The differences in IS policies and procedures are not as critical as the allocation of resources during an emergency, because both parties can agree on common standards and protocols for their disaster recovery operations, or they can adapt their policies and procedures to suit each other's needs. The maintenance of hardware and software compatibility is not as critical as the allocation of resources during an emergency, because both parties can use compatible or interoperable systems, or they can use virtualization or cloud computing technologies to overcome any compatibility issues. References: ISACA CISA Review Manual 27th Edition, page 281

NEW QUESTION 170
- (Topic 1)
Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

A. Audit cycle defined in the audit plan
B. Complexity of management's action plans
C. Recommendation from executive management
D. Residual risk from the findings of previous audits

Answer: D

Explanation:
Residual risk from the findings of previous audits should be the primary basis for prioritizing follow-up audits, because it reflects the level of exposure and potential impact that remains after management has implemented corrective actions or accepted the risk. Follow-up audits should focus on verifying whether the residual risk is within acceptable levels and whether the corrective actions are effective and sustainable. Audit cycle defined in the audit plan, complexity of management's action plans, and recommendation from executive management are not valid criteria for prioritizing follow-up audits, because they do not consider the residual risk from previous audits. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.4.3

NEW QUESTION 175
- (Topic 1)
Which of the following strategies BEST optimizes data storage without compromising data retention practices?

A. Limiting the size of file attachments being sent via email
B. Automatically deleting emails older than one year
C. Moving emails to a virtual email vault after 30 days
D. Allowing employees to store large emails on flash drives

Answer: A

Explanation:
The best strategy to optimize data storage without compromising data retention practices is to limit the size of file attachments being sent via email. This strategy can reduce the amount of storage space required for email messages, as well as the network bandwidth consumed by email traffic. File attachments can be large and often contain redundant or unnecessary information that can be compressed, converted, or removed before sending. By limiting the size of file attachments, the sender can encourage the use of more efficient formats, such as PDF or ZIP, or alternative methods of sharing files, such as cloud storage or web links. This can also improve the security and privacy of email communications, as large attachments may pose a higher risk of being intercepted, corrupted, or infected by malware.
References:
? Data Storage Optimization: What is it and Why Does it Matter?
? Data storage optimization 101: Everything you need to know

NEW QUESTION 177
- (Topic 1)
Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

A. business impact analysis (BIA).
B. threat and risk assessment.
C. business continuity plan (BCP).
D. disaster recovery plan (DRP).

Answer: C

Explanation:
A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A core part of a BCP is the documentation of workaround processes to keep a business function operational during recovery of IT systems. Workaround processes are alternative methods or procedures that can be used to perform a business function when the normal IT systems are unavailable or disrupted2. For example, if an online payment system is down, a workaround process could be to accept manual payments or use a backup system. Workaround processes help to minimize the impact of IT disruptions on the business operations and ensure continuity of service to customers and stakeholders3. References:
? 1 explains what is a business continuity plan and why it is important.
? 2 defines what is a workaround process and how it can be used in a BCP.
? 3 provides examples of workaround processes for different business functions.

NEW QUESTION 180
- (Topic 1)
An incorrect version of the source code was amended by a development team. This MOST likely indicates a weakness in:

A. incident management.
B. quality assurance (QA).
C. change management.
D. project management.

Answer: C

Explanation:
A weakness in change management is the most likely cause of an incorrect version of source code being amended by a development team. Change management is the process of controlling and documenting changes to IT systems and software. It ensures that changes are authorized, tested, and implemented in a controlled manner. If change management is weak, there is a risk of using outdated or incorrect versions of source code, which can lead to errors, defects, or security vulnerabilities in the software.

NEW QUESTION 181
- (Topic 1)
Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

A. Independent reconciliation
B. Re-keying of wire dollar amounts
C. Two-factor authentication control
D. System-enforced dual control

Answer: D

Explanation:
The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System-enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and recipients by different bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system. Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 182
- (Topic 1)
Which of the following is a social engineering attack method?

A. An unauthorized person attempts to gam access to secure premises by following an authonzed person through a secure door.
B. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone.
C. A hacker walks around an office building using scanning tools to search for a wireless network to gain access.
D. An intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties.

Answer: B

Explanation:
An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone. This is a social engineering attack method that exploits the trust or curiosity of the employee to obtain sensitive information that can be used to access or compromise the network. According to the web search results, social engineering is a technique that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information1. Phishing, whaling, baiting, and pretexting are some of the common forms of social engineering attacks2. Social engineering attacks are often more effective and profitable than purely technical attacks, as they rely on human error rather than system vulnerabilities

NEW QUESTION 183
- (Topic 1)
A proper audit trail of changes to server start-up procedures would include evidence of:

A. subsystem structure.
B. program execution.
C. security control options.
D. operator overrides.

Answer: D

Explanation:
A proper audit trail of changes to server start-up procedures would include evidence of operator overrides, which are actions taken by the system operator to bypass or modify the normal execution of the server start-up process. Operator overrides may indicate unauthorized or improper changes that could affect the security, availability, or performance of the server. Therefore, an audit trail should capture and document any operator overrides that occur during the server start-up process.
Evidence of subsystem structure, program execution, and security control options are not directly related to changes to server start-up procedures. Subsystem structure refers to the components and relationships of a subsystem within a larger system. Program execution refers to the process of running a software program on a computer. Security control options refer to the settings and parameters that define the security level and access rights for a system or application. These are all important aspects of auditing a server, but they do not provide evidence of changes to server start-up procedures.

NEW QUESTION 186
- (Topic 1)
When evaluating the design of controls related to network monitoring, which of the following is MOST important for an IS auditor to review?

A. Incident monitoring togs
B. The ISP service level agreement
C. Reports of network traffic analysis
D. Network topology diagrams

Answer: D

Explanation:
Network topology diagrams are the most important for an IS auditor to review when evaluating the design of controls related to network monitoring, because they show how the network components are connected and configured, and what security measures are in place to protect the network from unauthorized access or attacks. Incident monitoring logs, the ISP service level agreement, and reports of network traffic analysis are useful for evaluating the effectiveness and performance of network monitoring, but not the design of controls. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.3

NEW QUESTION 188
- (Topic 1)
Which of the following should be an IS auditor's GREATEST consideration when scheduling follow-up activities for agreed-upon management responses to remediate audit observations?

A. Business interruption due to remediation
B. IT budgeting constraints
C. Availability of responsible IT personnel
D. Risk rating of original findings

Answer: D

Explanation:
The most important consideration for an IS auditor when scheduling follow- up activities for agreed-upon management responses to remediate audit observations is the risk rating of original findings. The risk rating of original findings is an assessment of the potential impact or likelihood of an audit issue or observation on the organization's objectives, operations, or reputation. The risk rating of original findings can help determine the priority and urgency of follow-up activities for agreed-upon management responses to remediate audit observations by ensuring that high-risk issues are addressed first and more frequently than low-risk issues. The other options are not as important as the risk rating of original findings in scheduling follow-up activities for agreed-upon management responses to remediate audit observations, as they do not reflect the significance or severity of audit issues or observations. Business interruption due to remediation is a possible consequence of implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. IT budgeting constraints is a possible factor that may affect the availability or feasibility of resources for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. Availability of responsible IT personnel is a possible factor that may affect the accountability or responsiveness of staff for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION 191
- (Topic 1)
Which of the following is the BEST source of information for assessing the effectiveness of IT process monitoring?

A. Real-time audit software
B. Performance data
C. Quality assurance (QA) reviews
D. Participative management techniques

Answer: B

Explanation:
The best source of information for assessing the effectiveness of IT process monitoring is performance data. Performance data is a type of information that measures and reports on the results or outcomes of IT processes, such as availability, reliability, throughput, response time, or error rate. Performance data can help assess the effectiveness of IT process monitoring by providing quantitative and qualitative indicators of whether IT processes are meeting their objectives, standards, or expectations. The other options are not as good as performance data in assessing the effectiveness of IT process monitoring, as they do not provide direct or objective evidence of IT process results or outcomes. Real-time audit software is a type of tool that can help automate and facilitate audit activities, such as data collection, analysis, or reporting, but it does not provide information on IT process performance. Quality assurance (QA) reviews are a type of activity that can help evaluate and improve the quality of IT processes, products, or services, but they do not provide information on IT process performance. Participative management techniques are a type of method that can help involve and motivate IT staff in decision-making and problem-solving processes, but they do not provide information on IT process performance. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION 194
- (Topic 1)
Management is concerned about sensitive information being intentionally or unintentionally emailed as attachments outside the organization by employees. What is the MOST important task before implementing any associated email controls?

A. Require all employees to sign nondisclosure agreements (NDAs).
B. Develop an acceptable use policy for end-user computing (EUC).
C. Develop an information classification scheme.
D. Provide notification to employees about possible email monitoring.

Answer: C

Explanation:
The most important task before implementing any associated email controls to prevent sensitive information from being emailed outside the organization by employees is to develop an information classification scheme. An information classification scheme is a framework that defines the categories and levels of sensitivity for different types of information, such as public, internal, confidential, or secret. An information classification scheme can help implement email controls by providing criteria and guidelines for identifying, labeling, handling, and protecting sensitive information in email attachments. The other options are not as important as developing an information classification scheme, as they do not address the root cause of the problem or provide the same benefits. Requiring all employees to sign nondisclosure agreements (NDAs) is a legal control that can help deter or penalize employees from disclosing sensitive information, but it does not prevent them from emailing it outside the organization. Developing an acceptable use policy for end-user computing (EUC) is a governance control that can help define and communicate the rules and expectations for using IT resources, such as email, but it does not prevent employees from emailing sensitive information outside the organization. Providing notification to employees about possible email monitoring is a transparency control that can help inform and warn employees about the potential consequences of emailing sensitive information outside the organization, but it does not prevent them from doing so. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION 198

- (Topic 1)
During the evaluation of controls over a major application development project, the MOST effective use of an IS auditor's time would be to review and evaluate:

A. application test cases.
B. acceptance testing.
C. cost-benefit analysis.
D. project plans.

Answer: A

Explanation:
Reviewing and evaluating application test cases is the most effective use of an IS auditor's time during the evaluation of controls over a major application development project. Application test cases are designed to verify that the application meets the functional and non-functional requirements and specifications. They also help to identify and correct any errors, defects, or vulnerabilities in the application before it is deployed. By reviewing and evaluating the test cases, the IS auditor can assess the quality, reliability, security, and performance of the application and provide recommendations for improvement.

NEW QUESTION 200
- (Topic 3)
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

Answer: C

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. References: Accountability - ISACA, Audit Value - ISACA, Audit Follow- up - ISACA, Action Plan Consensus - ISACA, Factual Accuracy of Findings -
ISACA

NEW QUESTION 201
- (Topic 3)
Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

A. Limit check
B. Parity check
C. Reasonableness check
D. Validity check

Answer: D

Explanation:
The most likely application input control that would detect data input errors in the customer account number field during the processing of an accounts receivable transaction is a validity check. A validity check is a type of application control that verifies whether the data entered in an application matches a predefined set of values or criteria1. For example, a validity check can compare the customer account number entered by the user with a list of existing customer account numbers stored in a database, and reject any input that does not match any of the valid values2.
The other options are not as likely to detect data input errors in the customer account number field, because they do not compare the input with a predefined set of values or criteria. A limit check is a type of application control that verifies whether the data entered in an application falls within a specified range or limit1. For example, a limit check can ensure that the amount entered for an invoice does not exceed a certain maximum value2. A parity check is a type of application control that verifies whether the data entered in an application has an even or odd number of bits1. For example, a parity check can detect transmission errors in binary data by adding an extra bit to the data and checking whether the number of bits is consistent3. A reasonableness check is a type of application control that verifies whether the data entered in an application is logical or sensible based on other related data or information1. For example, a reasonableness check can ensure that the date entered for an order is not in the future or before the date of creation of the customer account2. References:
? What are application controls? Definition, examples & best practices1
? General Control Vs Application Control: Key Differences and Example …4
? Parity Check - an overview | ScienceDirect Topics

NEW QUESTION 202
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

* CISA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year