Isaca

Exam Questions CISA

Isaca CISA

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: D

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

NEW QUESTION 4
- (Topic 3)
Which of the following should be of GREATEST concern to an IS auditor reviewing a network printer disposal process?

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

Answer: B

Explanation:
The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been

sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 387

NEW QUESTION 5
- (Topic 3)
Which of the following is the BEST evidence that an organization's IT strategy is aligned lo its business objectives?

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

Answer: B

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

NEW QUESTION 6
- (Topic 3)
Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

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

Answer: D

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

NEW QUESTION 7
- (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 8
- (Topic 3)
An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

A. Increasing the frequency of risk-based IS audits for each business entity
B. Developing a risk-based plan considering each entity's business processes
C. Conducting an audit of newly introduced IT policies and procedures
D. Revising IS audit plans to focus on IT changes introduced after the split

Answer: B

Explanation:
Developing a risk-based plan considering each entity’s business processes would best help to ensure that IS audit still covers key risk areas within the IT

environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk-based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders1. By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope, and procedures accordingly. This can help to address the unique needs and expectations of each entity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance2.
The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Risk-Based Audit Planning: A Guide for Internal Audit1
? Risk-Based Audit Approach: Definition & Example

NEW QUESTION 9
- (Topic 3)
An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

A. deleted data cannot easily be retrieved.
B. deleting the files logically does not overwrite the files' physical data.
C. backup copies of files were not deleted as well.
D. deleting all files separately is not as efficient as formatting the hard disk.

Answer: B

Explanation:
An IS auditor should be concerned because deleting the files logically does not overwrite the files' physical data. Deleting a file from a hard disk only removes the reference or pointer to the file from the file system, but does not erase the actual data stored on the disk sectors. The deleted data can still be recovered using special tools or techniques until it is overwritten by new data. This poses a risk of data leakage, theft, or misuse if the hard disk falls into the wrong hands. To securely dispose of a system containing sensitive data, the hard disk should be wiped or sanitized using methods that overwrite or destroy the physical data beyond recovery. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 10
- (Topic 3)
An IS auditor finds that the process for removing access for terminated employees is not documented What is the MOST significant risk from this observation?

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

Answer: D

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

NEW QUESTION 10
- (Topic 3)
Which of the following should be the FRST step when developing a data toes prevention (DIP) solution for a large organization?

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

Answer: D

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

? ISACA CISA Review Manual 27th Edition (2019), page 247
? Data Loss Prevention—Next Steps - ISACA1
? What is data loss prevention (DLP)? | Microsoft Security

NEW QUESTION 11
- (Topic 3)
An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

A. reclassify the data to a lower level of confidentiality
B. require the business owner to conduct regular access reviews.
C. implement a strong password schema for users.
D. recommend corrective actions to be taken by the security administrator.

Answer: B

Explanation:
The best recommendation for an IS auditor who finds that one employee has unauthorized access to confidential data is to require the business owner to conduct regular access reviews. Access reviews are periodic assessments of user access rights and permissions to ensure that they are appropriate, necessary, and aligned with the business needs and objectives. Access reviews help to identify and remediate any unauthorized, excessive, or obsolete access that could pose a security risk or violate compliance requirements. The business owner is responsible for defining and approving the access requirements for their data and ensuring that they are enforced and monitored. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 16
- (Topic 3)
Which of the following is MOST critical for the effective implementation of IT governance?

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

Answer: C

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

NEW QUESTION 20
- (Topic 3)
An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

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

Answer: D

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

NEW QUESTION 22
- (Topic 3)
A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items lo the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

A. Separate authorization for input of transactions
B. Statistical sampling of adjustment transactions
C. Unscheduled audits of lost stock lines
D. An edit check for the validity of the inventory transaction

Answer: A

Explanation:
Separate authorization for input of transactions. This control would have best prevented this type of fraud in a retail environment by ensuring that the warehouse employee who handles the inventory items does not have the authority to enter adjustments to the inventory system. This would create a segregation of duties that would reduce the risk of collusion and concealment of theft.
The other options are not as effective as option A in preventing this type of fraud. Option B, statistical sampling of adjustment transactions, is a detective control that may help identify fraudulent transactions after they have occurred, but it does not prevent them from happening in the first place. Option C, unscheduled audits of lost stock lines, is also a detective control that may reveal discrepancies between the physical and recorded inventory, but it does not address the root cause of the fraud. Option D, an edit check for the validity of the inventory transaction, is a preventive control that may help verify the accuracy and completeness of the transaction data, but it does not prevent unauthorized or fraudulent adjustments.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Different Types of Inventory Fraud and How to Prevent Them1
? 6 Ways to Prevent Inventory Fraud in Your Business2

NEW QUESTION 25
- (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 26
- (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 27
- (Topic 3)
An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported the auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

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

Answer: C

Explanation:
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the

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

NEW QUESTION 32
- (Topic 3)
What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

A. The contract does not contain a right-to-audit clause.
B. An operational level agreement (OLA) was not negotiated.
C. Several vendor deliverables missed the commitment date.
D. Software escrow was not negotiated.

Answer: D

Explanation:
The greatest concern for an IS auditor reviewing contracts for licensed software that executes a critical business process is that software escrow was not negotiated. Software escrow is an arrangement where a third-party holds a copy of the source code and documentation of a licensed software in a secure location. The software escrow agreement specifies the conditions under which the licensee can access the escrowed materials, such as in case of bankruptcy, termination, or breach of contract by the licensor. Software escrow is important for ensuring the continuity and availability of a critical business process that depends on a licensed software. Without software escrow, the licensee may face significant risks and challenges in maintaining, modifying, or recovering the software in case of any disruption or dispute with the licensor. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 36
- (Topic 3)
Which of the following presents the GREATEST challenge to the alignment of business and IT?

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

Answer: A

Explanation:
The greatest challenge to the alignment of business and IT is the lack of chief information officer (CIO) involvement in board meetings. The CIO is the senior executive responsible for overseeing the IT strategy, governance, and operations of the organization, and ensuring that they support the business objectives and needs. The CIO should be involved in board meetings to communicate the value and contribution of IT to the organization, to align the IT vision and direction with the business strategy and priorities, and to advocate for the IT resources and investments required to achieve the desired outcomes. The lack of CIO involvement in board meetings can result in a disconnect between business and IT, a loss of trust and confidence in IT, and missed
opportunities for innovation and value creation. The other options are not as challenging as the lack of CIO involvement in board meetings, because they either do not affect the strategic alignment of business and IT, or they can be addressed by other means such as collaboration, negotiation, or escalation. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

NEW QUESTION 37
- (Topic 3)
During a follow-up audit, an IS auditor finds that some critical recommendations have the IS auditor's BEST course of action?

A. Require the auditee to address the recommendations in full.
B. Adjust the annual risk assessment accordingly.
C. Evaluate senior management's acceptance of the risk.
D. Update the audit program based on management's acceptance of risk.

Answer: C

Explanation:
The best course of action for an IS auditor who finds that some critical recommendations have not been implemented is to evaluate senior management’s acceptance of the risk. The IS auditor should understand the reasons why the recommendations have not been implemented and the implications for the organization’s risk exposure. The IS auditor should also verify that senior management has formally acknowledged and accepted the residual risk and has documented the rationale and justification for their decision. The IS auditor should communicate the findings and the risk acceptance to the audit committee and other relevant stakeholders. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 39
- (Topic 3)
Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

A. Temperature sensors
B. Humidity sensors
C. Water sensors
D. Air pressure sensors

Answer: C

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

NEW QUESTION 40
- (Topic 3)
Which of the following BEST describes an audit risk?

A. The company is being sued for false accusations.
B. The financial report may contain undetected material errors.
C. Employees have been misappropriating funds.
D. Key employees have not taken vacation for 2 years.

Answer: B

Explanation:
The best description of an audit risk is that the financial report may contain undetected material errors. Audit risk is the risk that the auditor expresses an inappropriate opinion on the financial report when it contains material misstatements or errors. Audit risk consists of three components: inherent risk, control risk, and detection risk. Inherent risk is the susceptibility of an assertion or a control to a material misstatement or error due to factors such as complexity, volatility, fraud, or human error. Control risk is the risk that a material misstatement or error will not be prevented or detected by the internal controls. 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. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 43
- (Topic 3)
An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which of two following is the MOST reliable follow- up procedure?

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

Answer: C

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

NEW QUESTION 44
- (Topic 3)
Which of the following is MOST important to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition?

A. Role-based access control policies
B. Types of data that can be uploaded to the platform
C. Processes for on-boarding and off-boarding users to the platform
D. Processes for reviewing administrator activity

Answer: B

Explanation:
The most important thing to determine during the planning phase of a cloud- based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization's policies and standards for data protection1.
The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired2. Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is acquired3. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the
platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established and performed after the platform is acquired4.
References:
? Cloud Messaging and Collaboration Services - Maryland.gov DoIT4
? MessageBird acquires real-time notifications and in-app messaging platform Pusher for $35M | TechCrunch2

? Symphony to lead financial market communications with the acquisition of Cloud9 Technologies3
? Cloud messaging and collaboration | Sumo Logic

NEW QUESTION 45
- (Topic 3)
During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed. Which of the following is the BEST way to help management understand the associated risk?

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

Answer: A

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

NEW QUESTION 50
- (Topic 3)
Which of the following BEST facilitates the legal process in the event of an incident?

A. Right to perform e-discovery
B. Advice from legal counsel
C. Preserving the chain of custody
D. Results of a root cause analysis

Answer: C

Explanation:
The best way to facilitate the legal process in the event of an incident is to preserve the chain of custody of the evidence. The chain of custody is a record of who handled, accessed, or modified the evidence, when, where, how, and why. The chain of custody helps to ensure the integrity, authenticity, and admissibility of the evidence in a court of law. The chain of custody also helps to prevent tampering, alteration, or loss of evidence that could compromise the investigation or the prosecution. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 55
- (Topic 3)
An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?

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

Answer: A

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

NEW QUESTION 59
- (Topic 3)
Which of the following would be MOST useful when analyzing computer performance?

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

Answer: A

Explanation:
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance,

it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
References:
? What is Computer Performance?
? How to Measure Computer Performance

NEW QUESTION 64
- (Topic 3)
An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which at the following is the BEST recommendation?

A. Implement key performance indicators (KPIs)
B. Implement annual third-party audits.
C. Benchmark organizational performance against industry peers.
D. Require executive management to draft IT strategy

Answer: A

Explanation:
The best recommendation for improving IT governance within the organization is to implement key performance indicators (KPIs). KPIs are measurable values that show how effectively the organization is achieving its key business objectives. KPIs can help the organization to monitor and evaluate the performance, efficiency, and alignment of its IT processes and resources with its business goals and strategies1.
The other options are not as effective as implementing KPIs for improving IT governance. Option B, implementing annual third-party audits, is a good practice but may not be sufficient or timely to identify and address the issues or gaps in IT governance. Option C, benchmarking organizational performance against industry peers, is a useful technique but may not reflect the specific needs and expectations of the organization's stakeholders. Option D, requiring executive management to draft IT strategy, is a necessary step but not enough to ensure that IT governance is implemented and monitored throughout the organization.

NEW QUESTION 68
- (Topic 3)
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

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

Answer: C

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

NEW QUESTION 72
- (Topic 3)
An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

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

Answer: A

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

NEW QUESTION 77
- (Topic 3)
A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

A. A formal request for proposal (RFP) process
B. Business case development procedures

C. An information asset acquisition policy
D. Asset life cycle management.

Answer: D

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

NEW QUESTION 78
- (Topic 3)
Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

A. Prepare detailed plans for each business function.
B. Involve staff at all levels in periodic paper walk-through exercises.
C. Regularly update business impact assessments.
D. Make senior managers responsible for their plan sections.

Answer: B

Explanation:
The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies1.
The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities2. Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks2. Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other2.
References:
? Best Practice Guide: Business Continuity Planning (BCP)3
? Best Practices for Creating a Business Continuity Plan1
? Business Continuity Plan Best Practices

NEW QUESTION 80
- (Topic 3)
An externally facing system containing sensitive data is configured such that users have either read-only or administrator rights. Most users of the system have administrator access. Which of the following is the GREATEST risk associated with this situation?

A. Users can export application logs.
B. Users can view sensitive data.
C. Users can make unauthorized changes.
D. Users can install open-licensed software.

Answer: C

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

NEW QUESTION 83
- (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 87
- (Topic 3)
Which of the following issues associated with a data center's closed-circuit television (CCTV) surveillance cameras should be of MOST concern to an IS auditor?

A. CCTV recordings are not regularly reviewed.
B. CCTV cameras are not installed in break rooms
C. CCTV records are deleted after one year.
D. CCTV footage is not recorded 24 x 7.

Answer: A

Explanation:
The most concerning issue associated with a data center’s CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and regulations. If the recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.
The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection. CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel. References:
? ISACA Journal Article: Physical security of a data center1
? Data Center Security: Checklist and Best Practices | Kisi2
? Video Surveillance Best Practices | Taylored Systems

NEW QUESTION 88
- (Topic 2)
An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

A. Data with customer personal information
B. Data reported to the regulatory body
C. Data supporting financial statements
D. Data impacting business objectives

Answer: B

Explanation:
To ensure that management concerns are addressed, internal audit should recommend that the data quality team review the data reported to the regulatory body first. This is because this data set is the most relevant and critical to the issue that triggered the enhancement of the data quality program. The data reported to the regulatory body should be accurate, complete, consistent, and timely, as any discrepancies could result in fines, penalties, or reputational damage for the organization. Data with customer personal information is important for data quality, but it is not directly related to the regulatory reporting issue. Data supporting financial statements is important for data quality, but it may not be the same as the data reported to the regulatory body. Data impacting business objectives is important for data quality, but it may not be as urgent or sensitive as the data reported to the regulatory body. References:
? CISA Review Manual, 27th Edition, pages 404-4051
? CISA Review Questions, Answers & Explanations Database, Question ID: 262

NEW QUESTION 92
- (Topic 2)
In a RAO model, which of the following roles must be assigned to only one individual?

A. Responsible
B. Informed
C. Consulted
D. Accountable

Answer: D

Explanation:
In a RAO model, which stands for Responsible, Accountable, Consulted, and Informed, the accountable role must be assigned to only one individual. The accountable role is the person who has the ultimate authority and responsibility for the outcome of the project or task, and who approves or rejects the work done by the responsible role. The accountable role cannot be delegated or shared, as it is essential to have a clear and single point of accountability for each project or task.
The other roles can be assigned to more than one individual:
? Responsible. This is the person who does the work or performs the task. There can be multiple responsible roles for different aspects or phases of a project or task, as long as they are coordinated and supervised by the accountable role.
? Informed. This is the person who needs to be notified or updated about the progress or results of the project or task. There can be multiple informed roles who have an interest or stake in the project or task, but who do not need to be consulted or involved in the decision-making process.
? Consulted. This is the person who provides input, feedback, or advice on the project or task. There can be multiple consulted roles who have expertise or

experience relevant to the project or task, but who do not have the authority or responsibility to approve or reject the work done by the responsible role.

NEW QUESTION 95
- (Topic 2)
Which of the following is the BEST reason for an organization to use clustering?

A. To decrease system response time
B. To Improve the recovery lime objective (RTO)
C. To facilitate faster backups
D. To improve system resiliency

Answer: D

Explanation:
Clustering is a technique that groups multiple servers or nodes together to act as one system, providing high availability, scalability, and load balancing for applications or services. Clustering can improve system resiliency, which is the ability of a system to withstand or recover from failures or disruptions without compromising its functionality or performance. Clustering can achieve this by providing redundancy and fault tolerance for critical components or processes, enabling automatic failover and recovery in case of node failures, distributing workload among multiple nodes to avoid overloading or bottlenecks, and allowing dynamic addition or removal of nodes to meet changing demand or capacity needs. Clustering may also decrease system response time by improving performance and efficiency through load balancing and parallel processing, but this is not its primary purpose. Clustering may facilitate faster backups by enabling concurrent backup operations across multiple nodes, but this is not its main benefit. Clustering may improve the recovery time objective (RTO), which is the maximum acceptable time for restoring a system or service after a disruption, by reducing the downtime and data loss caused by failures, but this is not the best reason for using clustering, as there may be other factors that affect the RTO, such as backup frequency, recovery procedures, and testing methods.

NEW QUESTION 100
- (Topic 2)
Which of the following documents should specify roles and responsibilities within an IT audit organization?

A. Organizational chart
B. Audit charier
C. Engagement letter
D. Annual audit plan

Answer: B

Explanation:
The audit charter is a document that defines the purpose, scope, authority, and responsibility of an IT audit organization. The audit charter should specify roles and responsibilities within an IT audit organization, such as who is accountable for approving the audit plan, who is responsible for conducting the audits, who is authorized to access the audit evidence, and who is accountable for reporting the audit results. The organizational chart, the engagement letter, and the annual audit plan are also important documents for an IT audit organization, but they do not specify roles and responsibilities as clearly and comprehensively as the audit charter.

NEW QUESTION 105
- (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 110
- (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 111
- (Topic 2)
The PRIMARY focus of a post-implementation review is to verify that:

A. enterprise architecture (EA) has been complied with.
B. user requirements have been met.
C. acceptance testing has been properly executed.
D. user access controls have been adequately designed.

Answer: B

Explanation:
The primary focus of a post-implementation review is to verify that user requirements have been met. User requirements are specifications that define what users need or expect from a system or service, such as functionality, usability, reliability, etc. User requirements are usually gathered and documented at the beginning of a project, and used as a basis for designing, developing, testing, and implementing a system or service. A post-implementation review is an evaluation that assesses whether a system or service meets its objectives and delivers its expected benefits after it has been implemented. The primary focus of a post-implementation review is to verify that user requirements have been met, as this can indicate whether the system or service satisfies the user needs and expectations, provides value and quality to the users, and supports the user goals and tasks. Enterprise architecture (EA) has been complied with is a possible focus of a post- implementation review, but it is not the primary one. EA is a framework that defines how an organization's business processes, information systems, and technology infrastructure are aligned and integrated to support its vision and strategy. EA has been complied with, as this can indicate whether the system or service fits with the organization's current and future state, and follows the organization's standards and principles. Acceptance testing has been properly executed is a possible focus of a post-implementation review, but it is not the primary one. Acceptance testing is a process that verifies whether a system or service meets the user requirements and expectations before it is accepted by the users or stakeholders. Acceptance testing has been properly executed, as this can indicate whether the system or service has been tested and validated by the users or stakeholders, and whether any issues or defects have been identified and resolved. User access controls have been adequately designed is a possible focus of a post-implementation review, but it is not the primary one. User access controls are mechanisms that ensure that only authorized users can access or use a system or service, and prevent unauthorized access or use. User access controls have been adequately designed, as this can indicate whether the system or service has appropriate security and privacy measures in place, and whether any risks or threats have been mitigated.

NEW QUESTION 112
- (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 114
- (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 117
- (Topic 2)
The waterfall life cycle model of software development is BEST suited for which of the following situations?

A. The protect requirements are wall understood.
B. The project is subject to time pressures.
C. The project intends to apply an object-oriented design approach.
D. The project will involve the use of new technology.

Answer: A

Explanation:
The waterfall life cycle model of software development is best suited for situations where the project requirements are well understood. The waterfall life cycle model is a sequential and linear approach to software development that consists of several phases, such as planning, analysis, design, implementation, testing, and maintenance. Each phase depends on the completion and approval of the previous phase before proceeding to the next phase. The waterfall life cycle model is best suited for situations where the project requirements are well understood, as it assumes that the requirements are clear, stable, and fixed at the beginning of the project, and do not change significantly throughout the project. The project is subject to time pressures is not a situation where the waterfall life cycle model of software development is best suited, as it may not be flexible or agile enough to accommodate changes or adjustments in the project schedule or timeline. The waterfall life cycle model may involve long delays or dependencies between phases, and may not allow for early feedback or delivery of software products. The project intends to apply an object-oriented design approach is not a situation where the waterfall life cycle model of software development is best suited, as it may not be compatible or effective with the object-oriented design approach. The object-oriented design approach is a technique that models software as a collection of interacting objects that have attributes and behaviors. The object-oriented design approach may require iterative and incremental development methods that allow for dynamic and adaptive changes in software design and functionality. The project will involve the use of new technology is not a situation where the waterfall life cycle model of software development is best suited, as it may not be able to cope with the uncertainty or complexity of new technology. The waterfall life cycle model may not allow for sufficient exploration or experimentation with new technology, and may not be able to handle changes or issues that arise from new technology.

NEW QUESTION 118
- (Topic 2)
The IS quality assurance (OA) group is responsible for:

A. ensuring that program changes adhere to established standards.
B. designing procedures to protect data against accidental disclosure.
C. ensuring that the output received from system processing is complete.
D. monitoring the execution of computer processing tasks.

Answer: A

Explanation:
The IS quality assurance (QA) group is responsible for ensuring that program changes adhere to established standards. Program changes are modifications made to software applications or systems to fix errors, improve performance, add functionality, or meet changing requirements. Program changes should follow established standards for documentation, authorization, testing, implementation, and review. The IS QA group is responsible for verifying that program changes comply with these standards and meet the expected quality criteria. Designing procedures to protect data against accidental disclosure; ensuring that the output received from system processing is complete; and monitoring the execution of computer processing tasks are not responsibilities of the IS QA group. References: [ISACA CISA Review Manual 27th Edition], page 304.

NEW QUESTION 122
- (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 125
- (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 129
- (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 132
- (Topic 2)
Which of the following is MOST important for an IS auditor to verify when evaluating an organization's firewall?

A. Logs are being collected in a separate protected host
B. Automated alerts are being sent when a risk is detected
C. Insider attacks are being controlled
D. Access to configuration files Is restricted.

Answer: A

Explanation:
A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can help protect an organization’s network and information systems from unauthorized or malicious access, by filtering or blocking unwanted or harmful packets. The most important thing for an IS auditor to verify when evaluating an organization’s firewall is that the logs are being collected in a separate protected host. Logs are records of events or activities that occur on a system or network, such as connections, requests, responses, errors, and alerts. Logs can provide valuable information for auditing, monitoring, troubleshooting, and investigating security incidents. However, logs can also be tampered with, deleted, or corrupted by attackers or insiders who want to hide their tracks or evidence of their actions. Therefore, it is essential that logs are stored in a separate host that is isolated and secured from the network and the firewall itself, to prevent unauthorized access or modification of the logs. Automated alerts are being sent when a risk is detected is a good practice for enhancing the security and efficiency of a firewall, but it is not the most important thing for an IS auditor to verify, as alerts may not always be accurate, timely, or actionable. Insider attacks are being controlled is a desirable outcome for a firewall, but it is not the most important thing for an IS auditor to verify, as insider attacks may involve other factors or methods that bypass or compromise the firewall, such as social engineering, credential theft, or physical access. Access to configuration files is restricted is a critical control for ensuring the security and integrity of a firewall, but it is not the most important thing for an IS auditor to verify, as configuration files may not reflect the actual state or performance of the firewall.

NEW QUESTION 135
- (Topic 2)
A now regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor’s BEST recommendation to facilitate compliance with the regulation?

A. Establish key performance indicators (KPIs) for timely identification of security incidents.
B. Engage an external security incident response expert for incident handling.
C. Enhance the alert functionality of the intrusion detection system (IDS).
D. Include the requirement in the incident management response plan.

Answer: D

Explanation:
The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.
The other options are not as effective as including the requirement in the incident management response plan:
? Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the

regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.
? Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.
? Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

NEW QUESTION 139
- (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 143
- (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 146
- (Topic 2)
Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm tor potential software vulnerabilities?

A. Guest operating systems are updated monthly
B. The hypervisor is updated quarterly.
C. A variety of guest operating systems operate on one virtual server
D. Antivirus software has been implemented on the guest operating system only.

Answer: D

Explanation:
Antivirus software has been implemented on the guest operating system only is the observation that an IS auditor would consider the greatest risk when conducting an audit of a virtual server farm for potential software vulnerabilities. A virtual server farm is a collection of servers that run multiple virtual machines (VMs) on a single physical host using a software layer called a hypervisor. A guest operating system is the operating system installed on each VM. Antivirus software is a software program that detects and removes malicious software from a computer system. If antivirus software has been implemented on the guest operating system only, it means that the hypervisor and the host operating system are not protected from malware attacks, which could compromise the security and availability of all VMs running on the same host. Therefore, antivirus software should be implemented on both the guest and host operating systems as well as on the hypervisor. References: CISA Review Manual, 27th Edition, page 378

NEW QUESTION 147
- (Topic 2)
An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

A. There Is a reconciliation process between the spreadsheet and the finance system
B. A separate copy of the spreadsheet is routinely backed up
C. The spreadsheet is locked down to avoid inadvertent changes
D. Access to the spreadsheet is given only to those who require access

Answer: D

Explanation:
Access to the spreadsheet is given only to those who require access is the most important control for maintaining the security of data in the spreadsheet. An IS auditor should ensure that the principle of least privilege is applied to limit the access to sensitive financial data and prevent unauthorized disclosure, modification, or deletion. The other options are less important controls that may enhance the accuracy, availability, or integrity of data in the spreadsheet, but not its security.
References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.31
? CISA Review Questions, Answers & Explanations Database, Question ID 210

NEW QUESTION 150
- (Topic 2)
Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist within the organization?

A. Reviewing vacation patterns
B. Reviewing user activity logs
C. Interviewing senior IT management
D. Mapping IT processes to roles

Answer: D

Explanation:
Mapping IT processes to roles is an activity that provides an IS auditor with the most insight regarding potential single person dependencies that might exist within the organization. Single person dependencies occur when only one person has the knowledge, skills, or access rights to perform a critical IT function. Mapping IT processes to roles can help to identify such dependencies and assess their impact on the continuity and security of IT operations. The other activities do not provide as much insight into single person dependencies, as they do not show the relationship between IT processes and roles. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION 153
- (Topic 2)
Which of the following is MOST helpful for measuring benefits realization for a new system?

A. Function point analysis
B. Balanced scorecard review
C. Post-implementation review
D. Business impact analysis (BIA)

Answer: C

Explanation:
This is the most helpful method for measuring benefits realization for a new system, because it involves evaluating the actual outcomes and impacts of the system after it has been implemented and used for a certain period of time. A post-implementation review can compare the actual benefits with the expected benefits that were defined in the business case or the benefits realization plan, and identify any gaps, issues, or opportunities for improvement. A post-implementation review can also assess the effectiveness, efficiency, and satisfaction of the system's users, stakeholders, and customers, and provide feedback and recommendations for future enhancements or changes.
The other options are not as helpful as post-implementation review for measuring benefits realization for a new system:
? Function point analysis. This is a technique that measures the size and complexity
of a software system based on the number and types of functions it provides. Function point analysis can help estimate the cost, effort, and time required to develop, maintain, or enhance a software system, but it does not measure the actual benefits or value that the system delivers to the organization or its users.
? Balanced scorecard review. This is a strategic management tool that measures the
performance of an organization or a business unit based on four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard review can help align the organization's vision, mission, and goals with its activities and outcomes, but it does not measure the specific benefits or impacts of a new system.
? Business impact analysis (BIA). This is a process that identifies and evaluates the potential effects of a disruption or disaster on the organization's critical business functions and processes. A BIA can help determine the recovery priorities, objectives, and strategies for the organization in case of an emergency, but it does not measure the benefits or value of a new system.

NEW QUESTION 157
- (Topic 2)
A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon The MOST effective plan of action would be to:

A. evaluate replacement systems and performance monitoring software.
B. restrict functionality of system monitoring software to security-related events.
C. re-install the system and performance monitoring software.
D. use analytical tools to produce exception reports from the system and performance monitoring software

Answer: D

Explanation:
Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective plan of action for a company that purchased and implemented system and performance monitoring software. Exception reports are reports that highlight deviations or anomalies from predefined thresholds or standards. Using analytical tools to produce exception reports can help to reduce the size and complexity of the system and performance monitoring reports, as well as to focus on the most relevant and critical information for review and action. The other options are less effective plans of action, as they may involve unnecessary costs, risks, or efforts. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
? CISA Review Questions, Answers & Explanations Database, Question ID 219

NEW QUESTION 160
- (Topic 2)

Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS audit has been asked to conduct a control assessment. the auditor's BEST course of action would be to determine if:

A. the patches were updated.
B. The logs were monitored.
C. The network traffic was being monitored.
D. The domain controller was classified for high availability.

Answer: B

Explanation:
The auditor's best course of action after a security breach in which a hacker exploited a well-known vulnerability in the domain controller is to determine if the logs were monitored. Log monitoring is an essential control for detecting and responding to security incidents, especially when known vulnerabilities exist in the system. The auditor should assess if the logs were properly configured, collected, reviewed, analyzed, and acted upon by the responsible parties. Updating patches, monitoring network traffic, and classifying domain controllers for high availability are also important controls, but they are not directly related to the detection and response of the security breach. References:
? CISA Review Manual (Digital Version), page 301
? CISA Questions, Answers & Explanations Database, question ID 3340

NEW QUESTION 163
- (Topic 2)
When testing the adequacy of tape backup procedures, which step BEST verifies that regularly scheduled Backups are timely and run to completion?

A. Observing the execution of a daily backup run
B. Evaluating the backup policies and procedures
C. Interviewing key personnel evolved In the backup process
D. Reviewing a sample of system-generated backup logs

Answer: D

Explanation:
Reviewing a sample of system-generated backup logs is the best step to verify that regularly scheduled backups are timely and run to completion. Backup logs are records that document the details and results of backup operations, such as the date, time, duration, status, errors, and exceptions. By reviewing a sample of backup logs, the IS auditor can check whether the backups are performed according to the schedule and whether they are completed successfully or not. The other steps do not provide as much evidence or assurance as reviewing backup logs, as they do not show the actual outcome or performance of backup operations. References: CISA Review Manual, 27th Edition, page 247

NEW QUESTION 164
- (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 168
- (Topic 2)
Which of the following is a social engineering attack method?

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

Answer: A

Explanation:
Social engineering is a technique that exploits human weaknesses, such as trust, curiosity, or greed, to obtain information or access from a target. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone is an example of a social engineering attack method, as it involves manipulating the employee into divulging sensitive information that can be used to compromise the network or system. A hacker walks around an office building using scanning tools to search for a wireless network to gain access, an intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties, and an unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door are not examples of social engineering attack methods, as they do not involve human interaction or deception. References: [ISACA CISA Review Manual 27th Edition], page 361.

NEW QUESTION 171
- (Topic 2)
Which of the following is the GREATEST risk associated with storing customer data on a web server?

A. Data availability
B. Data confidentiality
C. Data integrity
D. Data redundancy

Answer: B

Explanation:
The greatest risk associated with storing customer data on a web server is data confidentiality. Data confidentiality is the property that ensures that data are accessible only to authorized entities or individuals, and protected from unauthorized disclosure or exposure. Storing customer data on a web server poses a high risk to data confidentiality, as web servers are exposed to the internet and may be vulnerable to various types of attacks or breaches that can compromise the security and privacy of customer data, such as hacking, phishing, malware, denial of service (DoS), etc. Customer data may contain sensitive or personal information that can cause harm or damage to customers or the organization if disclosed or exposed, such as identity theft, fraud, reputation loss, legal liability, etc. Data availability is the property that ensures that data are accessible and usable by authorized entities or individuals when needed. Data availability is a risk associated with storing customer data on a web server, as web servers may experience failures or disruptions that can affect the accessibility and usability of customer data, such as hardware faults, network issues, power outages, etc. However, data availability is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data integrity is the property that ensures that data are accurate and consistent, and protected from unauthorized modification or corruption. Data integrity is a risk associated with storing customer data on a web server, as web servers may be subject to attacks or errors that can affect the accuracy and consistency of customer data, such as injection attacks, tampering, replication issues, etc. However, data integrity is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data redundancy is the condition of having duplicate or unnecessary data in a database or system. Data redundancy is not a risk associated with storing customer data on a web server, but rather a result of poor database design or management.

NEW QUESTION 172
- (Topic 2)
To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

A. Review IT staff job descriptions for alignment
B. Develop quarterly training for each IT staff member.
C. Identify required IT skill sets that support key business processes
D. Include strategic objectives m IT staff performance objectives

Answer: C

Explanation:
Identifying required IT skill sets that support key business processes is the first step to enable the alignment of IT staff development plans with IT strategy. An IT strategy is a plan that defines how IT will support the organization's goals and objectives. Identifying required IT skill sets means determining the knowledge, abilities, and competencies that IT staff need to perform their roles and responsibilities effectively and efficiently. This can help to align IT staff development plans with IT strategy, as well as to identify and address any skill gaps or needs within the IT workforce. The other options are not the first steps to enable alignment, but rather possible subsequent actions that may depend on the required IT skill sets. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.11
? CISA Review Questions, Answers & Explanations Database, Question ID 229

NEW QUESTION 175
- (Topic 2)
Which of the following BEST enables the timely identification of risk exposure?

A. External audit review
B. Internal audit review
C. Control self-assessment (CSA)
D. Stress testing

Answer: C

Explanation:
Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References:
ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION 176
- (Topic 2)
Stress testing should ideally be earned out under a:

A. test environment with production workloads.
B. production environment with production workloads.
C. production environment with test data.
D. test environment with test data.

Answer: A

Explanation:
Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:

? CISA Review Manual, 27th Edition, pages 471-4721
? CISA Review Questions, Answers & Explanations Database, Question ID: 261

NEW QUESTION 179
- (Topic 2)
An IS auditor concludes that an organization has a quality security policy. Which of the following is MOST important to determine next? The policy must be:

A. well understood by all employees.
B. based on industry standards.
C. developed by process owners.
D. updated frequently.

Answer: A

Explanation:
The most important thing to determine next after concluding that an organization has a quality security policy is whether the policy is well understood by all employees. A security policy is a document that defines the objectives, scope, roles, responsibilities, and rules for information security within an organization. A quality security policy is one that is clear, concise, consistent, comprehensive, and aligned with business goals and requirements. However, a quality security policy is useless if it is not well understood by all employees who are expected to comply with it. Therefore, the IS auditor should assess the level of awareness and understanding of the security policy among employees and identify any gaps or issues that need to be addressed. The other options are not as important as ensuring that the security policy is well understood by all employees, as they do not directly affect the implementation and effectiveness of the security policy.
References: CISA Review Manual, 27th Edition, page 317

NEW QUESTION 184
- (Topic 2)
Which of the following business continuity activities prioritizes the recovery of critical functions?

A. Business continuity plan (BCP) testing
B. Business impact analysis (BIA)
C. Disaster recovery plan (DRP) testing
D. Risk assessment

Answer: B

Explanation:
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects or consequences of disruptions or disasters on an organization's critical business functions or processes. A BIA can help prioritize the recovery of critical functions by assessing their importance and urgency for the organization's operations, objectives, and stakeholders, and determining their recovery time objectives (RTOs), which are the maximum acceptable time for restoring a function after a disruption. A business continuity plan (BCP) testing is a process that verifies and validates the effectiveness and readiness of a BCP, which is a document that outlines the strategies and procedures for ensuring the continuity of critical business functions in the event of a disruption or disaster. A BCP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are recovered according to the BCP. A disaster recovery plan (DRP) testing is a process that verifies and validates the effectiveness and readiness of a DRP, which is a document that outlines the technical and operational steps for restoring the IT systems and infrastructure that support critical business functions in the event of a disruption or disaster. A DRP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are supported by the IT systems and infrastructure according to the DRP. A risk assessment is a process that identifies and analyzes the potential threats and vulnerabilities that could affect an organization's critical business functions or processes. A risk assessment does not prioritize the recovery of critical functions, but rather estimates their likelihood and impact of being disrupted by various risk scenarios.

NEW QUESTION 185
- (Topic 2)
A third-party consultant is managing the replacement of an accounting system. Which of the following should be the IS auditor's GREATEST concern?

A. Data migration is not part of the contracted activities.
B. The replacement is occurring near year-end reporting
C. The user department will manage access rights.
D. Testing was performed by the third-party consultant

Answer: C

Explanation:
The greatest concern for an IS auditor in this scenario is that the user department will manage access rights to the new accounting system. This could pose a significant risk of unauthorized access, segregation of duties violations, data tampering and fraud. The IS auditor should ensure that access rights are defined, approved and monitored by an independent function, such as IT security or internal audit. The other options are not as concerning as option C, as they can be mitigated by other controls or procedures. Data migration is an important part of the system replacement project, but it can be performed by another party or verified by the IS auditor. The timing of the replacement near year-end reporting is a challenge, but it can be managed by proper planning, testing and contingency plans. Testing performed by the third-party consultant is acceptable, as long as it is reviewed and validated by the IS auditor or another independent party.
References: CISA Review Manual (Digital Version) 1, Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.4: System Implementation.

NEW QUESTION 186
- (Topic 2)
An IS auditor is reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents. Which of the following observations should be of MOST concern to the auditor?

A. Training was not provided to the department that handles intellectual property and patents
B. Logging and monitoring for content filtering is not enabled.
C. Employees can share files with users outside the company through collaboration tools.
D. The collaboration tool is hosted and can only be accessed via an Internet browser

Answer: B

Explanation:
The observation that should be of most concern to the auditor when reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents is that employees can share files with users outside the company through collaboration tools. Collaboration tools are software or hardware devices that enable users to communicate, cooperate, and coordinate with each other on a common task or project. Collaboration tools can facilitate information sharing and knowledge exchange among users, but they can also pose security risks if not properly controlled or managed. Employees can share files with users outside the company through collaboration tools, as this can compromise the security and confidentiality of intellectual property and patents, which are valuable and sensitive assets of the organization. Employees may share files with unauthorized or untrusted users who may misuse or disclose the intellectual property and patents, either intentionally or unintentionally. This can cause harm or damage to the organization, such as loss of competitive advantage, reputation, revenue, or legal rights. Training was not provided to the department that handles intellectual property and patents is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Training is an activity that educates and instructs users on how to use collaboration tools effectively and securely,
such as how to access, share, store, and protect information using collaboration tools. Training was not provided to the department that handles intellectual property and patents, as this can affect the awareness and competence of users on collaboration tools, and increase the likelihood of errors or mistakes that may compromise the security or quality of information. However, this observation may not be directly related to collaboration tools, as it may apply to any information system or resource used by the department. Logging and monitoring for content filtering is not enabled is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Logging and monitoring are processes that record and analyze the events or activities that occur on an information system or network, such as user actions, system operations, data changes, errors, alerts, etc. Content filtering is a technique that blocks or allows access to certain types of information based on predefined criteria or rules, such as keywords, categories, sources, etc. Logging and monitoring for content filtering is not enabled, as this can affect the auditability, accountability, and visibility of collaboration tools, and prevent detection or investigation of security incidents or violations related to information sharing using collaboration tools. However, this observation may not be specific to collaboration tools, as it may affect any information system or network that uses content filtering. The collaboration tool is hosted and can only be accessed via an Internet browser is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. A hosted collaboration tool is a type of cloud-based service that provides collaboration functionality over the Internet without requiring installation or maintenance on local devices. An Internet browser is a software application that enables users to access and interact with web-based content or services. The collaboration tool is hosted and can only be accessed via an Internet browser, as this can affect the availability and reliability of collaboration tools, and introduce security or privacy risks for information sharing using collaboration tools. However, this observation may not be unique to collaboration tools, as it may apply to any cloud-based service that uses an Internet browser.

NEW QUESTION 188
- (Topic 2)
Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

A. The person who collected the evidence is not qualified to represent the case.
B. The logs failed to identify the person handling the evidence.
C. The evidence was collected by the internal forensics team.
D. The evidence was not fully backed up using a cloud-based solution prior to the trial.

Answer: B

Explanation:
The evidence collected during a digital forensic investigation would not be admissible in court if the logs failed to identify the person handling the evidence. This would violate the chain of custody principle, which requires that the evidence be properly documented, secured, and tracked throughout the investigation process. The chain of custody ensures that the evidence is authentic, reliable, and trustworthy, and that it has not been tampered with or altered. The person who collected the evidence, whether qualified or not, is not relevant to the admissibility of the evidence, as long as they followed the proper procedures and protocols. The evidence collected by the internal forensics team can be admissible in court, as long as they are independent, objective, and competent. The evidence does not need to be fully backed up using a cloud-based solution prior to the trial, as long as it is preserved and protected from damage or loss. References: ISACA Journal Article: Digital Forensics: Chain of Custody

NEW QUESTION 192
- (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 196

- (Topic 2)
An organization has developed mature risk management practices that are followed across all departments What is the MOST effective way for the audit team to leverage this risk management maturity?

A. Implementing risk responses on management's behalf
B. Integrating the risk register for audit planning purposes
C. Providing assurances to management regarding risk
D. Facilitating audit risk identification and evaluation workshops

Answer: B

Explanation:
The most effective way for the audit team to leverage the risk management maturity of the organization is to integrate the risk register for audit planning purposes. The risk register is a document that records the identified risks, their likelihood, impact, and mitigation strategies for a project or an organization. By using the risk register, the audit team can align their audit objectives, scope, and procedures with the organization's risk profile and priorities. This will help the audit team to provide more value-added and relevant assurance and recommendations to the management and stakeholders.
Some of the web sources that support this answer are:
? Audit Maturity And Risk Management | Ideagen
? Building a Mature Enterprise Risk Management Plan | AuditBoard
? CISA Certified Information Systems Auditor – Question0551

NEW QUESTION 201
.....

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

https://www.exambible.com/CISA-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/