Exam Questions CISA

Isaca CISA

https://www.2passeasy.com/dumps/CISA/

NEW QUESTION 1
- (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 2
- (Topic 3)
Which of the following should be performed FIRST before key performance indicators (KPIs) can be implemented?

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

Answer: B

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

NEW QUESTION 3
- (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 4
- (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 5
- (Topic 3)
Which of the following should be the IS auditor's PRIMARY focus, when evaluating an organization's offsite storage facility?

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

Answer: B

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

NEW QUESTION 6
- (Topic 3)
An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business The auditor's PRIMARY concern would be:

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

Answer: B

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

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

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

Answer: A

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

NEW QUESTION 9
- (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 10
- (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 10
- (Topic 3)
An organization allows its employees lo use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

A. Installing security software on the devices
B. Partitioning the work environment from personal space on devices
C. Preventing users from adding applications
D. Restricting the use of devices for personal purposes during working hours

Answer: B

Explanation:
Partitioning the work environment from personal space on devices. This would best maintain information security without compromising employee privacy by creating a separate and secure area on the personal mobile devices for work-related data and applications. This way, the organization can protect its information from unauthorized access, loss, or leakage, while respecting the employees' personal data and preferences on their own devices.
The other options are not as effective as option B in balancing information security and employee privacy. Option A, installing security software on the devices, is a good practice but may not be sufficient to prevent data breaches or comply with regulatory requirements. Option C, preventing users from adding applications, is too restrictive and may interfere with the employees' personal use of their devices. Option D, restricting the use of devices for personal purposes during working hours, is impractical and difficult to enforce. References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Personal Cellphone Privacy at Work1
? Protecting your personal information and privacy on a company phone2
? Mobile Devices and Protected Health Information (PHI)3
? Using your personal phone for work? Here's how to separate your apps and data4
? 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

NEW QUESTION 14

- (Topic 3)
An IS auditor reviewing the threat assessment tor a data center would be MOST concerned if:

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

Answer: C

Explanation:
An IS auditor reviewing the threat assessment for a data center would be most concerned if the exercise was completed by local management, because this could introduce bias, conflict of interest, or lack of expertise in the assessment process. A threat assessment is a systematic method of identifying and evaluating the potential threats that could affect the availability, integrity, or confidentiality of the data center and its assets. A threat assessment should be conducted by an independent and qualified team that has the necessary skills, knowledge, and experience to perform a comprehensive and objective analysis of the data center's environment, vulnerabilities, and risks1.
The other options are not as concerning as option C for an IS auditor reviewing the threat assessment for a data center. Option A, some of the identified threats are unlikely to occur, is not a problem as long as the likelihood and impact of each threat are properly estimated and prioritized. A threat assessment should consider all possible scenarios, even if they have a low probability of occurrence, to ensure that the data center is prepared for any eventuality2. Option B, all identified threats relate to external entities, is not a flaw as long as the assessment also considers internal threats, such as human errors, malicious insiders, or equipment failures. External threats are often more visible and severe than internal threats, but they are not the only source of risk for a data center3. Option D, neighboring organizations' operations have been included, is not a mistake as long as the assessment also focuses on the data center's own operations. Neighboring organizations' operations may have an impact on the data center's security and availability, especially if they share physical or network infrastructure or resources. A threat assessment should take into account the interdependencies and interactions between the data center and its external environment4.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Data Center Threats and Vulnerabilities1
? Datacenter threat, vulnerability, and risk assessment2
? Data Centre Risk Assessment3

NEW QUESTION 15
- (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 19
- (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 24

- (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 26
- (Topic 3)
Which of the following is necessary for effective risk management in IT governance?

A. Local managers are solely responsible for risk evaluation.
B. IT risk management is separate from corporate risk management.
C. Risk management strategy is approved by the audit committee.
D. Risk evaluation is embedded in management processes.

Answer: D

Explanation:
The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 29
- (Topic 3)
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA> to automate routine business tasks?

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

Answer: A

Explanation:
The most important thing for an IS auditor to confirm when reviewing an organization’s plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures12. Without a proper documentation of the end-to-end process, the organization may face challenges in designing, developing, testing, deploying, and monitoring the RPA solution3. References:
1: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211 2: CISA Online Review Course, Module 4: Information Systems Operations and Business
Resilience, Lesson 4.2: IT Service Delivery and Support 3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

NEW QUESTION 34
- (Topic 3)
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?

A. Analyze a new application that moots the current re
B. Perform an analysis to determine the business risk
C. Bring the escrow version up to date.
D. Develop a maintenance plan to support the application using the existing code

Answer: C

Explanation:
This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version. This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements. Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version

of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application.
An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application1.
The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time-consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application2. Option B, performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk3. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code. References:
? How Important Is Source Code Escrow - ISACA1
? The What and Why of Source Code Escrow2
? Unlocking Source Code In Escrow 2023: A Guide To Secure Software3

NEW QUESTION 35
- (Topic 3)
An IS auditor follows up on a recent security incident and finds the incident response was not adequate. Which of the following findings should be considered MOST critical?

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

Answer: A

Explanation:
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.
The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 254
? Incident Response Process - ISACA1
? Incident Response: How to Identify and Fix Security Weaknesses

NEW QUESTION 37
- (Topic 3)
Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

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

Answer: B

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

NEW QUESTION 40
- (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 44
- (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 45
- (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 50
- (Topic 3)
An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

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

Answer: C

Explanation:
The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies. Security parameters are settings or options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization's policies are documents that define the security goals, requirements, standards, and guidelines for the organization's information systems. An IS auditor should verify that security parameters are set in accordance with the organization's policies to ensure that the new server complies with the organization's security expectations and regulations. The other options are less important or incorrect because:
? A. Security parameters should not be set in accordance with the manufacturer's standards alone, as they may not reflect the organization's specific security

needs and environment. The manufacturer's standards are general recommendations or best practices for configuring the server's security parameters based on common scenarios and threats. An IS auditor should compare the manufacturer's standards with the organization's policies and identify any gaps or conflicts that need to be resolved.
? B. A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.
? D. The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization. References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA], [Business Case- ISACA], [Tender - ISACA], [Procurement Management - ISACA]

NEW QUESTION 55
- (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 59
- (Topic 3)
The PRIMARY role of a control self-assessment (CSA) facilitator is to:

A. conduct interviews to gain background information.
B. focus the team on internal controls.
C. report on the internal control weaknesses.
D. provide solutions for control weaknesses.

Answer: B

Explanation:
The primary role of a control self-assessment (CSA) facilitator is to focus the team on internal controls. A CSA facilitator is a person who guides the CSA process and helps the participants to identify, assess, and improve their internal controls. The facilitator does not conduct interviews, report on weaknesses, or provide solutions, as these are the responsibilities of the participants themselves1.
The other options are incorrect because they are not the primary role of a CSA facilitator. Option A, conduct interviews to gain background information, is a preliminary step that may be done by the facilitator or the participants before the CSA session, but it is not the main purpose of the facilitator. Option C, report on the internal control weaknesses, is an outcome of the CSA process that should be done by the participants who own and operate the controls. Option D, provide solutions for control weaknesses, is also an outcome of the CSA process that should be done by the participants who are in charge of implementing the improvements.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019, page 2822
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066693
? PwC, Control Self Assessments4
? Workiva, 4 factors of an effective control self-assessment (CSA) program5

NEW QUESTION 64
- (Topic 3)
Which of the following is the BEST way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC)?

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

Answer: B

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

NEW QUESTION 69
- (Topic 3)
An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the

application back in- house. Which of the following findings should be the IS auditor's GREATEST concern?

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

Answer: D

Explanation:
The finding that should be the IS auditor's greatest concern is that the data model is not clearly documented. A data model is a representation of the structure, relationships, and constraints of the data used by an application. It is a vital component of the software development process, as it helps to ensure the accuracy, consistency, and quality of the data1. A clear and comprehensive documentation of the data model is essential for the maintenance and support of the application, as it facilitates the understanding, modification, and troubleshooting of the data and the application logic2.
If the organization plans to bring the support and future maintenance of the application back in-house, it will need to have access to the data model documentation from the vendor. Without it, the organization may face difficulties in transferring the knowledge and skills from the vendor to the in-house team, as well as in adapting and enhancing the application to meet changing business needs and requirements3. The lack of data model documentation may also increase the risk of errors, inconsistencies, and inefficiencies in the data and the application performance2.
The other findings are not as concerning as the lack of data model documentation, because they do not directly affect the quality and maintainability of the application. The cost of outsourcing is lower than in-house development is a benefit rather than a risk for the organization, as it implies that outsourcing has helped to save time and money for the organization4. The vendor development team is located overseas is a common practice in outsourcing, and it does not necessarily imply a lower quality or a higher risk of the application. However, it may pose some challenges in terms of communication, coordination, and cultural differences, which can be managed by establishing clear expectations, roles, and responsibilities, as well as using effective tools and methods for communication and collaboration5. A training plan for business users has not been developed is a gap that should be addressed by the organization before deploying the application, as it may affect the user acceptance and satisfaction of the application. However, it does not directly impact the quality or maintainability of the application itself. References:
? What is Data Modeling? Definition & Types | Informatica1
? Data Modeling Best Practices: Documentation | erwin2
? Data Model Documentation - an overview | ScienceDirect Topics3
? Outsourcing App Development Pros and Cons – Droids On Roids4
? 8 Risks of Software Development Outsourcing & Their Solutions - Acropolium5
? Software Training Plan: How to Create One for Your Business - Elinext

NEW QUESTION 73
- (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 75
- (Topic 3)
Which of the following is the BEST metric to measure the alignment of IT and business strategy?

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

Answer: B

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

NEW QUESTION 80
- (Topic 3)
Which of the following would BEST help to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software?

A. Assign the security risk analysis to a specially trained member of the project management office.
B. Deploy changes in a controlled environment and observe for security defects.
C. Include a mandatory step to analyze the security impact when making changes.

D. Mandate that the change analyses are documented in a standard format.

Answer: C

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

NEW QUESTION 85
- (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 89
- (Topic 3)
Which of the following is MOST important when planning a network audit?

A. Determination of IP range in use
B. Analysis of traffic content
C. Isolation of rogue access points
D. Identification of existing nodes

Answer: D

Explanation:
The most important factor when planning a network audit is to identify the existing nodes on the network. Nodes are devices or systems that are connected to the network and can communicate with each other. Nodes can include servers, workstations, routers, switches, firewalls, printers, scanners, cameras, etc. Identifying the existing nodes on the network will help the auditor to determine the scope, objectives, and methodology of the audit. It will also help the auditor to assess the network topology, architecture, performance, security, and compliance. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 92
- (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 94
- (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 96
- (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 97
- (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 98
- (Topic 3)
Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

A. Restricting evidence access to professionally certified forensic investigators
B. Documenting evidence handling by personnel throughout the forensic investigation
C. Performing investigative procedures on the original hard drives rather than images of the hard drives
D. Engaging an independent third party to perform the forensic investigation

Answer: B

Explanation:
The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation. Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time, location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the investigation. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 101
- (Topic 3)
Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's disaster recovery plan (DRP)?

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

Answer: C

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

NEW QUESTION 102
- (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 103
- (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)
Which of the following BEST protects an organization's proprietary code during a joint- development activity involving a third party?

A. Statement of work (SOW)
B. Nondisclosure agreement (NDA)
C. Service level agreement (SLA)
D. Privacy agreement

Answer: B

Explanation:
A nondisclosure agreement (NDA) is the best way to protect an organization's proprietary code during a joint-development activity involving a third party. An NDA is a legal contract that binds the parties involved in a joint-development activity to keep confidential any information, data or materials that are shared or exchanged during the activity. An NDA specifies what constitutes confidential information, how it can be used, disclosed or protected, how long it remains confidential, what are the exceptions and remedies for breach of confidentiality, and other terms and conditions. An NDA can help to protect an organization's proprietary code from being copied, modified, distributed or exploited by unauthorized parties without its consent or knowledge. The other options are not as effective as option B, as they do not address confidentiality issues specifically. A statement of work (SOW) is a document that defines the scope, objectives, deliverables, tasks, roles, responsibilities, timelines and costs of a joint-development activity, but it does not cover confidentiality issues explicitly. A service level agreement (SLA) is a document that defines the quality, performance and availability standards and metrics for a service provided by one party to another party in a joint-development activity, but it does not cover confidentiality issues explicitly. A privacy agreement is a document that defines how personal information collected from customers or users is collected, used, disclosed and protected by one party or both parties in a joint-development activity, but it does not cover confidentiality issues related to proprietary code. References: CISA Review Manual (Digital Version) , Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.2: Project Management Practices.

NEW QUESTION 108
- (Topic 2)
Which of the following would be an appropriate rote of internal audit in helping to establish an organization's privacy program?

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

Answer: A

Explanation:
Analyzing risks posed by new regulations is an appropriate role of internal audit in helping to establish an organization's privacy program. An internal auditor can provide assurance and advisory services on the compliance and effectiveness of the privacy program, as well as identify and assess the potential risks and impacts of new or changing privacy regulations. The other options are not appropriate roles of internal audit, but rather the responsibilities of the management, the information security officer, or the privacy officer. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
? CISA Review Questions, Answers & Explanations Database, Question ID 216

NEW QUESTION 110
- (Topic 2)
Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

A. Data from the source and target system may be intercepted.
B. Data from the source and target system may have different data formats.
C. Records past their retention period may not be migrated to the new system.
D. System performance may be impacted by the migration

Answer: A

Explanation:
The greatest security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system is data from the source and target system may be intercepted. Data interception is an attack that occurs when an unauthorized entity or individual captures or accesses data that are being transmitted or stored on an information system or network. Data interception can compromise the confidentiality and integrity of data, and cause harm or damage to data owners or users. Data migration from a legacy HR system to a cloud-based system involves transferring data from one system or location to another system or location over a network connection. This poses a high risk of data interception, as data may be exposed or vulnerable during transit or storage on unsecured or untrusted networks or systems. Data from the source and target system may have different data formats is a possible challenge associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. Data formats are specifications that define how data are structured or encoded on an information system or network. Data formats may vary depending on different systems or platforms. Data migration may require converting data from one format to another format to ensure compatibility and interoperability between systems. Records past their retention period may not be migrated to the new system is a possible outcome associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. Retention period is a duration that defines how long data should be kept or stored on an information system or network before being deleted or destroyed. Retention period may depend on various factors such as legal requirements, business needs, storage capacity, etc. Data migration may involve deleting or destroying data that are past their retention period to reduce the volume or complexity of data to be transferred or to comply with regulations or policies. System performance may be impacted by the migration is a possible impact associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. System performance is a measure of how well an information system or network functions or operates, such as speed, reliability, availability, etc. System performance may be affected by data migration, as data migration may consume significant resources or bandwidth, cause interruptions or delays, or introduce errors or inconsistencies.

NEW QUESTION 115
- (Topic 2)
Which of the following is MOST important to verify when determining the completeness of the vulnerability scanning process?

A. The organization's systems inventory is kept up to date.
B. Vulnerability scanning results are reported to the CISO.
C. The organization is using a cloud-hosted scanning tool for Identification of vulnerabilities
D. Access to the vulnerability scanning tool is periodically reviewed

Answer: A

Explanation:
The completeness of the vulnerability scanning process depends on the accuracy and currency of the organization's systems inventory, which is a list of all the hardware and software assets that are owned or used by the organization. A complete and up-to-date systems inventory can help ensure that all the systems are identified and scanned for vulnerabilities, and that no system is missed or overlooked. Vulnerability scanning results are reported to the CISO is a good practice for

ensuring accountability and visibility of the vulnerability management process, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as reporting does not guarantee that all the systems are scanned. The organization is using a cloud-hosted scanning tool for identification of vulnerabilities is a possible option for conducting vulnerability scanning, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as the type of scanning tool does not affect the scope or coverage of the scanning. Access to the vulnerability scanning tool is periodically reviewed is a critical control for ensuring the security and integrity of the vulnerability scanning tool, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as access review does not ensure that all the systems are scanned.

NEW QUESTION 118
- (Topic 2)
Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

A. Historical privacy breaches and related root causes
B. Globally accepted privacy best practices
C. Local privacy standards and regulations
D. Benchmark studies of similar organizations

Answer: C

Explanation:
The best source of information for an IS auditor to use as a baseline to assess the adequacy of an organization’s privacy policy is the local privacy standards and regulations. Privacy standards and regulations are legal requirements that specify how personal data should be collected, processed, stored, shared, and disposed of by organizations. By using local privacy standards and regulations as a baseline, the IS auditor can ensure that the organization’s privacy policy complies with the applicable laws and protects the rights and interests of data subjects. Historical privacy breaches and related root causes, globally accepted privacy best practices, and benchmark studies of similar organizations are useful sources of information for improving an organization’s privacy policy, but they are not as authoritative and relevant as local privacy standards and regulations. References: CISA Review Manual (Digital Version): Chapter 2 - Governance and Management of Information Technology

NEW QUESTION 121
- (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 123
- (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 125
- (Topic 2)
Which of the following BEST Indicates that an incident management process is effective?

A. Decreased time for incident resolution
B. Increased number of incidents reviewed by IT management

C. Decreased number of calls lo the help desk
D. Increased number of reported critical incidents

Answer: A

Explanation:
Decreased time for incident resolution is the best indicator that an incident management process is effective. Incident management is a process that aims to restore normal service operation as quickly as possible after an incident, which is an unplanned interruption or reduction in quality of an IT service. Decreased time for incident resolution means that the incident management process is able to identify, analyze, respond to, and resolve incidents efficiently and effectively. The other indicators do not necessarily reflect the effectiveness of the incident management process, as they may depend on other factors such as the nature, frequency, and severity of incidents. References: CISA Review Manual, 27th Edition, page 372

NEW QUESTION 127
- (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 129
- (Topic 2)
When auditing the alignment of IT to the business strategy, it is MOST Important for the IS auditor to:

A. compare the organization's strategic plan against industry best practice.
B. interview senior managers for their opinion of the IT function.
C. ensure an IT steering committee is appointed to monitor new IT projects.
D. evaluate deliverables of new IT initiatives against planned business services.

Answer: D

Explanation:
When auditing the alignment of IT to the business strategy, it is most important for the IS auditor to evaluate deliverables of new IT initiatives against planned business services. This can help the IS auditor to assess whether the IT initiatives are meeting the business needs and expectations, delivering value and benefits, and supporting the business objectives and goals. Comparing the organization’s strategic plan against industry best practice is a possible technique for auditing the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as industry best practice may not be applicable or relevant to the specific context or situation of the organization. Interviewing senior managers for their opinion of the IT function is a possible technique for auditing the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as senior managers’ opinions may be subjective or biased, and may not reflect the actual performance or outcomes of the IT function. Ensuring an IT steering committee is appointed to monitor new IT projects is a possible control for ensuring the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as an IT steering committee may not be effective or efficient in monitoring new IT projects, and may not have sufficient authority or influence over the IT function.

NEW QUESTION 133
- (Topic 2)
Which of the following is MOST important to consider when scheduling follow-up audits?

A. The efforts required for independent verification with new auditors
B. The impact if corrective actions are not taken
C. The amount of time the auditee has agreed to spend with auditors
D. Controls and detection risks related to the observations

Answer: B

Explanation:
The impact if corrective actions are not taken is the most important factor to consider when scheduling follow-up audits. An IS auditor should prioritize the follow-up audits based on the risk and potential consequences of not addressing the audit findings and recommendations. The other options are less important factors that may affect the timing and scope of the follow-up audits, but not their necessity or urgency. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
? CISA Review Questions, Answers & Explanations Database, Question ID 207

NEW QUESTION 136
- (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 139
- (Topic 2)
Which of the following environments is BEST used for copying data and transformation into a compatible data warehouse format?

A. Testing
B. Replication
C. Staging
D. Development

Answer: C

Explanation:
The best environment for copying data and transforming it into a compatible data warehouse format is the staging environment. The staging environment is a temporary area where data from various sources are extracted, transformed, and loaded (ETL) before being moved to the data warehouse. The staging environment allows for data cleansing, validation, integration, and standardization without affecting the source or target systems. The testing environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for verifying and validating the functionality and performance of applications or systems. The replication environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating identical copies of data or systems for backup or recovery purposes. The development environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating or modifying applications or systems. References:
? CISA Review Manual, 27th Edition, pages 475-4761
? CISA Review Questions, Answers & Explanations Database, Question ID: 2642

NEW QUESTION 142
- (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)
Which of the following findings from an IT governance review should be of GREATEST concern?

A. The IT budget is not monitored
B. All IT services are provided by third parties.
C. IT value analysis has not been completed.
D. IT supports two different operating systems.

Answer: C

Explanation:
IT value analysis has not been completed is a finding from an IT governance review that should be of greatest concern. IT value analysis is a process of measuring and demonstrating the contribution of IT to the organization's goals and objectives. An IS auditor should be concerned about the lack of IT value analysis, as it may indicate that the IT investments and resources are not aligned with the business needs and expectations, or that the IT performance and outcomes are not monitored and evaluated. The other options are less critical findings that may not have a significant impact on the IT governance. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.11
? CISA Review Questions, Answers & Explanations Database, Question ID 218

NEW QUESTION 149

- (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 152
- (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 156
- (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 160
- (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 161
- (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 163
- (Topic 2)
Which of the following is the MOST important activity in the data classification process?

A. Labeling the data appropriately
B. Identifying risk associated with the data
C. Determining accountability of data owners
D. Determining the adequacy of privacy controls

Answer: C

Explanation:
Determining accountability of data owners is the most important activity in the data classification process. Data classification is a process that assigns categories or labels to data based on their value, sensitivity, criticality and risk to the organization. Data classification helps to determine the appropriate level of protection, access and retention for data. Determining accountability of data owners is an activity that identifies and assigns roles and responsibilities for data classification, protection and management to individuals or functions within the organization. Data owners are individuals or functions who have authority and responsibility for defining, classifying, protecting and managing data throughout their lifecycle. Determining accountability of data owners is essential for ensuring that data are classified correctly and consistently, and that data classification policies and procedures are followed and enforced. The other options are not as important as option C, as they are dependent on or derived from the accountability of data owners. Labeling the data appropriately is an activity that applies the categories or labels assigned by data owners to data based on their classification criteria. Identifying risk associated with the data is an activity that assesses the potential impact and likelihood of loss, disclosure, modification or destruction of data based on their classification level. Determining the adequacy of privacy controls is an activity that evaluates whether the controls implemented to protect personal or sensitive data are sufficient and effective based on their classification level. References: CISA Review Manual (Digital Version) , Chapter 5: Protection of Information Assets, Section 5.3: Data Classification.

NEW QUESTION 165
- (Topic 2)
The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

A. the access control system's log settings.
B. how the latest system changes were implemented.
C. the access control system's configuration.
D. the access rights that have been granted.

Answer: D

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

NEW QUESTION 167
- (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 168
- (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 171
- (Topic 2)
In an online application which of the following would provide the MOST information about the transaction audit trail?

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

Answer: C

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

NEW QUESTION 175
- (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 180
- (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 182
- (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 183
- (Topic 2)
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

A. Perform substantive testing of terminated users' access rights.
B. Perform a review of terminated users' account activity
C. Communicate risks to the application owner.
D. Conclude that IT general controls ate ineffective.

Answer: B

Explanation:
The IS auditor's next step after determining that many terminated users' accounts were not disabled is to perform a review of terminated users' account activity. This means that the IS auditor should check whether any of the terminated users' accounts were accessed or used after their termination date, which could indicate unauthorized or fraudulent activity. The IS auditor should also assess the impact and risk of such activity on the confidentiality, integrity, and availability of IT resources and data. The other options are not as appropriate as performing a review of terminated users' account activity, as they do not provide sufficient evidence or assurance of the extent and effect of the problem.
References: CISA Review Manual, 27th Edition, page 240

NEW QUESTION 186
- (Topic 2)
An IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer payments. The IS auditor should FIRST

A. document the exception in an audit report.
B. review security incident reports.
C. identify compensating controls.
D. notify the audit committee.

Answer: C

Explanation:
The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:
? CISA Review Manual, 27th Edition, pages 295-2961
? CISA Review Questions, Answers & Explanations Database, Question ID: 260

NEW QUESTION 191
- (Topic 2)
An employee loses a mobile device resulting in loss of sensitive corporate data. Which o(the following would have BEST prevented data leakage?

A. Data encryption on the mobile device
B. Complex password policy for mobile devices
C. The triggering of remote data wipe capabilities
D. Awareness training for mobile device users

Answer: A

Explanation:
The best way to prevent data leakage from a lost mobile device is data encryption on the mobile device. Data encryption is a technique that transforms data into an unreadable format using a secret key or algorithm. Data encryption protects data from unauthorized access or disclosure in case of loss or theft of a mobile device. Complex password policy for mobile devices, triggering of remote data wipe capabilities, and awareness training for mobile device users are useful measures to enhance data security on mobile devices, but they do not prevent data leakage as effectively as data encryption. A complex password policy can be bypassed by brute force attacks or password cracking tools. Remote data wipe capabilities depend on network connectivity and device power availability. Awareness training for mobile device users can reduce human errors or negligence, but it cannot guarantee compliance or behavior change. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 195
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISA Product From:

https://www.2passeasy.com/dumps/CISA/

Money Back Guarantee

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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