Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (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 2
- (Topic 3)
Which of the following would be an appropriate role of internal audit in helping to establish an organization’s privacy program?

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

Answer: A

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

NEW QUESTION 3
- (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 4
- (Topic 3)
During the planning phase of a data loss prevention (DLP) audit, management expresses a concern about mobile computing. Which of the following should the IS auditor identity as the associated risk?

A. The use of the cloud negatively impacting IT availably

B. Increased need for user awareness training
C. Increased vulnerability due to anytime, anywhere accessibility
D. Lack of governance and oversight for IT infrastructure and applications

Answer: C

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

NEW QUESTION 5
- (Topic 3)
An IS auditor notes that the previous year's disaster recovery test was not completed within the scheduled time frame due to insufficient hardware allocated by a third-party vendor. Which of the following provides the BEST evidence that adequate resources are now allocated to successfully recover the systems?

A. Service level agreement (SLA)
B. Hardware change management policy
C. Vendor memo indicating problem correction
D. An up-to-date RACI chart

Answer: A

Explanation:
The best evidence that adequate resources are now allocated to successfully recover the systems is a service level agreement (SLA). An SLA is a contract between a service provider and a customer that defines the scope, quality, and terms of the service delivery. An SLA should include measurable and verifiable indicators of the service performance, such as availability, reliability, capacity, security, and recovery. An SLA should also specify the roles, responsibilities, and expectations of both parties, as well as the remedies and penalties for non-compliance. An SLA can help to ensure that the third- party vendor has allocated sufficient hardware and other resources to meet the recovery objectives and requirements of the organization. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 6
- (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 7
- (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 8
- (Topic 3)
Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

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

Answer: B

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

NEW QUESTION 9
- (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 10
- (Topic 3)
What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

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

Answer: D

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

NEW QUESTION 10
- (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 11
- (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 14
- (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 16
- (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 18
- (Topic 3)
Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

A. IT steering committee minutes
B. Business objectives
C. Alignment with the IT tactical plan
D. Compliance with industry best practice

Answer: B

Explanation:
The most important consideration for an IS auditor when assessing the adequacy of an organization’s information security policy is the business objectives. An information security policy is a document that defines the organization’s approach to protecting its information assets from internal and external threats. It should align with the organization’s mission, vision, values, and goals, and support its business processes and functions1. An information security policy should also be focused on the business needs and requirements of the organization, rather than on technical details or specific solutions2. The other options are not as important as the business objectives, because they do not directly reflect the organization’s purpose and direction. IT steering committee minutes are records of the discussions and decisions made by a group of senior executives who oversee the IT strategy and governance of the organization. They may provide some insights into the information security policy, but they are not sufficient to evaluate its adequacy3. Alignment with the IT tactical plan is a measure of how well the information security policy supports the short-term actions and projects that implement the IT strategy. However, the IT tactical plan itself should be aligned with the business objectives, and not vice versa4. Compliance with industry best practice is a desirable quality of an information security policy, but it is not a guarantee of its effectiveness or suitability for the organization. Industry best practices are general guidelines or recommendations that may not apply to every organization or situation. An information security policy should be customized and tailored to the specific context and needs of the organization. References:
? The 12 Elements of an Information Security Policy | Exabeam1
? 11 Key Elements of an Information Security Policy | Egnyte2
? What is an IT steering committee? Definition, roles & responsibilities …3
? What is IT Strategy? Definition, Components & Best Practices | BMC …4
? IT Security Policy: Key Components & Best Practices for Every Business

NEW QUESTION 23
- (Topic 3)
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

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

Answer: C

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

NEW QUESTION 25
- (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 27
- (Topic 3)
The PRIMARY objective of value delivery in reference to IT governance is to:

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

Answer: C

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

NEW QUESTION 30
- (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 34
- (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 38
- (Topic 2)
An organization has recently implemented a Voice-over IP (VoIP) communication system. Which ot the following should be the IS auditor's PRIMARY concern?

A. A single point of failure for both voice and data communications
B. Inability to use virtual private networks (VPNs) for internal traffic
C. Lack of integration of voice and data communications
D. Voice quality degradation due to packet toss

Answer: A

Explanation:
The IS auditor’s primary concern when an organization has recently implemented a Voice-over IP (VoIP) communication system is a single point of failure for both voice and data communications. VoIP is a technology that allows voice communication over IP networks such as the internet. VoIP can offer benefits such as lower costs, higher flexibility, and better integration with other applications. However, VoIP also introduces risks such as dependency on network availability, performance, and security. If both voice and data communications share the same network infrastructure and devices, then a single point of failure can affect both services simultaneously and cause significant disruption to business operations. Therefore, the IS auditor should evaluate the availability and redundancy of the network components and devices that support VoIP communication. The other options are not as critical as a single point of failure for both voice and data communications, as they do not pose a direct threat to business continuity. References: CISA Review Manual, 27th Edition, page 385

NEW QUESTION 41
- (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 43
- (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 45
- (Topic 2)
An internal audit department recently established a quality assurance (QA) program. Which of the following activities Is MOST important to include as part of the QA program requirements?

A. Long-term Internal audit resource planning
B. Ongoing monitoring of the audit activities
C. Analysis of user satisfaction reports from business lines
D. Feedback from Internal audit staff

Answer: B

Explanation:

Ongoing monitoring of the audit activities is the most important activity to include as part of the quality assurance (QA) program requirements for an internal audit department. An IS auditor should perform regular reviews and evaluations of the audit processes, methods, standards, and outcomes to ensure that they comply with the QA program objectives and criteria. This will help to maintain and improve the quality and consistency of the audit services and deliverables. The other options are less important activities to include as part of the QA program requirements, as they may involve long-term resource planning, user satisfaction reports, or feedback from internal audit staff. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.61
? CISA Review Questions, Answers & Explanations Database, Question ID 224

NEW QUESTION 46
- (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 48
- (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 51
- (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 55
- (Topic 2)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

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

NEW QUESTION 59
- (Topic 2)
Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist within the organization?

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

Answer: D

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

NEW QUESTION 61
- (Topic 2)
Which of the following is MOST helpful for measuring benefits realization for a new system?

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

Answer: C

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

NEW QUESTION 66
- (Topic 2)
An IS auditor is evaluating the risk associated with moving from one database management system (DBMS) to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

A. Preserving the same data classifications
B. Preserving the same data inputs
C. Preserving the same data structure
D. Preserving the same data interfaces

Answer: C

Explanation:
The most helpful thing to ensure the integrity of the system throughout the change when moving from one database management system (DBMS) to another is preserving the same data structure. A DBMS is a software system that manages and manipulates data stored in a database, such as creating, updating, querying, deleting, etc. A database is a collection of structured or organized data that can be accessed or manipulated by a DBMS. A data structure is a way of organizing or arranging data in a database, such as tables, columns, rows, keys, indexes, etc. Preserving the same data structure when moving from one DBMS to another can help ensure the integrity of the system throughout the change, by maintaining the consistency and accuracy of data in the database, and avoiding any errors or issues that may arise from incompatible or inconsistent data structures between different DBMSs. Preserving the same data classifications is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data classifications are categories or labels that define the level of sensitivity or importance of data in a database, such as public, confidential, secret, etc. Data classifications can help protect the security and privacy of data in the database by applying appropriate controls or restrictions on data access or use based on their classifications.

Preserving the same data classifications when moving from one DBMS to another can help ensure the integrity of the system throughout the change by preventing unauthorized or inappropriate access or use of data in the database. However, this may not be directly related to the DBMS change, as it may apply to any data migration or transfer process. Preserving the same data inputs is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data inputs are sources or methods that provide data to a database, such as user inputs, sensors, files, etc. Data inputs can affect the quality and validity of data in the database by introducing errors or inconsistencies in data entry or collection. Preserving the same data inputs when moving from one DBMS to another can help ensure the integrity of the system throughout the change by reducing errors or inconsistencies in data input or collection.

NEW QUESTION 67
- (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 68
- (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 72
- (Topic 2)
Stress testing should ideally be earned out under a:

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

Answer: A

Explanation:
Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:
? CISA Review Manual, 27th Edition, pages 471-4721
? CISA Review Questions, Answers & Explanations Database, Question ID: 261

NEW QUESTION 76
- (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 80
- (Topic 2)
Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

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

Answer: B

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

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

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

Answer: D

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

NEW QUESTION 85
- (Topic 2)
Which of the following is the BEST way for an organization to mitigate the risk associated with third-party application performance?

A. Ensure the third party allocates adequate resources to meet requirements.
B. Use analytics within the internal audit function
C. Conduct a capacity planning exercise
D. Utilize performance monitoring tools to verify service level agreements (SLAs)

Answer: D

Explanation:
The best way for an organization to mitigate the risk associated with third- party application performance is to utilize performance monitoring tools to verify service level agreements (SLAs). Performance monitoring tools are software or hardware devices that measure and report the performance of an application or system, such as speed, availability, reliability, etc. Performance monitoring tools can help mitigate the risk associated with third-party application performance, by allowing the organization to verify whether the third-party provider is meeting the SLAs, which are contracts or agreements that define the expected level and quality of service for an application or system. Performance monitoring tools can also help identify and resolve any performance issues or problems that may arise from the third-party application. Ensuring the third party allocates adequate resources to meet requirements is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be feasible or effective depending on the availability, cost, and suitability of the resources. Using analytics within the internal audit function is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be timely or relevant depending on the frequency, scope, and quality of the analytics. Conducting a capacity planning exercise is a possible way to

mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be accurate or reliable depending on the assumptions, methods, and data used for the capacity planning.

NEW QUESTION 86
- (Topic 2)
An organization has developed mature risk management practices that are followed across all departments What is the MOST effective way for the audit team to leverage this risk management maturity?

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

Answer: B

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

NEW QUESTION 88
- (Topic 2)
An IS auditor notes that IT and the business have different opinions on the availability of their application servers. Which of the following should the IS auditor review FIRST in order to understand the problem?

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

Answer: A

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

NEW QUESTION 91
- (Topic 2)
Which of the following is a detective control?

A. Programmed edit checks for data entry
B. Backup procedures
C. Use of pass cards to gain access to physical facilities
D. Verification of hash totals

Answer: D

Explanation:
Verification of hash totals is a detective control. A detective control is a control that aims to identify and report errors or irregularities that have already occurred. Verification of hash totals is a technique that compares the hash values of data before and after transmission or processing to detect any changes or corruption. The other options are examples of other types of controls, such as programmed edit checks (preventive), backup procedures (recovery), and use of pass cards (preventive). References: CISA Review Manual, 27th Edition, page 223

NEW QUESTION 96
- (Topic 2)
A manager Identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor In this scenario?

A. Terminated staff
B. Unauthorized access
C. Deleted log data
D. Hacktivists

Answer: A

Explanation:
A threat actor is an entity or individual that poses a potential harm or danger to an organization's information systems or data. Terminated staff are the threat actors in this scenario, as they are former employees who may still have active privileged accounts that grant them access to sensitive or critical information or resources of the organization. Terminated staff may abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of the information systems or data, either intentionally or unintentionally. Unauthorized access is a threat event or action that occurs when an unauthorized entity or individual gains access to an organization's information systems or data without permission or authorization. Unauthorized access is not a threat actor, but rather

a result of a threat actor's activity. Deleted log data is a threat consequence or impact that occurs when log data, which are records of events or activities that occur on an information system or network, are erased or corrupted by a threat actor. Deleted log data can affect the auditability, accountability, and visibility of the information system or network, and prevent detection or investigation of security incidents. Deleted log data is not a threat actor, but rather a result of a threat actor's activity. Hacktivists are threat actors who use hacking techniques to promote a political or social cause or agenda. Hacktivists are not the threat actors in this scenario, as there is no indication that they are involved in this case.

NEW QUESTION 97
- (Topic 2)
Which of the following represents the HIGHEST level of maturity of an information security program?

A. A training program is in place to promote information security awareness.
B. A framework is in place to measure risks and track effectiveness.
C. Information security policies and procedures are established.
D. The program meets regulatory and compliance requirements.

Answer: B

Explanation:
According to the ISACA's Information Security Governance Guidance for Boards of Directors and Executive Management, the highest level of maturity of an information security program is Level 5: Optimized, which means that the program is aligned with the business objectives and strategy, and continuously monitors and improves its performance and effectiveness. A framework is in place to measure risks and track effectiveness, and the program is proactive, adaptive, and innovative. The other options represent lower levels of maturity:
? A training program is in place to promote information security awareness. This is Level 2: Repeatable, which means that the program has some basic policies and procedures, and provides awareness training to employees.
? Information security policies and procedures are established. This is Level 3:
Defined, which means that the program has formalized policies and procedures, and assigns roles and responsibilities for information security.
? The program meets regulatory and compliance requirements. This is Level 4:
Managed, which means that the program has established metrics and reporting mechanisms, and complies with relevant laws and regulations.
References: : ISACA. (2001). Information Security Governance Guidance for B

NEW QUESTION 102
- (Topic 2)
An IS auditor is analyzing a sample of accesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found Which sampling method would be appropriate?

A. Discovery sampling
B. Judgmental sampling
C. Variable sampling
D. Stratified sampling

Answer: A

Explanation:
Discovery sampling is an appropriate sampling method for an IS auditor who intends to launch an intensive investigation if one exception is found. Discovery sampling is a type of attribute sampling that determines the sample size based on an acceptable risk of not finding at least one occurrence of an attribute when a given rate of occurrence exists in a population. Discovery sampling can be used by an IS auditor who wants to detect fraud or errors that have a low probability but high impact on an audit objective. The other options are not appropriate sampling methods for this purpose, as they may involve judgmental sampling, variable sampling, or stratified sampling. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 230

NEW QUESTION 103
- (Topic 2)
Which of the following types of firewalls provide the GREATEST degree of control against hacker intrusion?

A. Circuit gateway
B. Application level gateway
C. Packet filtering router
D. Screening router

Answer: B

Explanation:
The type of firewall that provides the greatest degree of control against hacker intrusion is an application level gateway. A firewall is a device or software that filters or blocks network traffic based on predefined rules or policies. A firewall can help protect an information system or network from unauthorized access or attack by hackers or other malicious entities. An application level gateway is a type of firewall that operates at the application layer of the network model (layer 7), which is where user applications communicate with each other over the network. An application level gateway provides the greatest degree of control against hacker intrusion, by inspecting and analyzing the content and context of each network packet at the application level, such as protocols, commands, requests, responses, etc., and allowing or denying access based on specific criteria or conditions. An application level gateway can also perform additional functions such as authentication, encryption, caching, logging, etc., to enhance the security and performance of network traffic. A circuit gateway is a type of firewall that operates at the transport layer of the network model (layer 4), which is where data are transferred between end points over the network. A circuit gateway provides a moderate degree of control against hacker intrusion by establishing a secure connection between two end points (such as client and server) and relaying network packets between them without inspecting or analyzing their content. A circuit gateway can also perform functions such as encryption, authentication, or address translation to improve the security and privacy of network traffic. A packet filtering router is a type of firewall that operates at the network layer of the network model (layer 3), which is where data are routed between different networks or subnets. A packet filtering router provides a low degree of control against hacker intrusion by examining the header of each network packet and allowing or denying access based on basic criteria such as source address, destination address, port number, protocol, etc. A packet filtering router can also perform functions such as routing, forwarding, or address translation to optimize the delivery and efficiency of network traffic. A screening router is a type of firewall that operates at the network layer of the network model (layer 3), which is where data are routed between different networks or subnets. A screening router provides a low degree of control against hacker intrusion by examining the header of each network packet and allowing or denying access based on basic criteria such as source address, destination address, port number, protocol, etc. A screening router can also perform

functions such as routing, forwarding, or address translation to optimize the delivery and efficiency of network traffic.

NEW QUESTION 104
- (Topic 2)
An IS auditor is reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit. What should the auditor consider the MOST significant concern?

A. Attack vectors are evolving for industrial control systems.
B. There is a greater risk of system exploitation.
C. Disaster recovery plans (DRPs) are not in place.
D. Technical specifications are not documented.

Answer: B

Explanation:
The most significant concern for an IS auditor when reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit is that there is a greater risk of system exploitation. System exploitation is an attack that occurs when an unauthorized entity or individual takes advantage of a vulnerability or weakness in a system to compromise its security or functionality. System exploitation can cause harm or damage to the system or its users, such as data loss, corruption, theft, manipulation, denial of service (DoS), etc. An ICS that uses older unsupported technology poses a high risk of system exploitation, as older technology may have known or unknown vulnerabilities or defects that have not been patched or fixed by the vendor or manufacturer, and unsupported technology may not receive any updates or support from the vendor or manufacturer in case of issues or incidents. Attack vectors are evolving for industrial control systems is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Attack vectors are methods or pathways that attackers use to gain access to or attack a system. Attack vectors are evolving for industrial control systems, as attackers are developing new techniques or tools to target ICSs that are increasingly connected and complex. However, this concern may not be specific to older unsupported technology, as it may affect any ICS regardless of its technology level. Disaster recovery plans (DRPs) are not in place is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. DRPs are documents that outline the technical and operational steps for restoring the IT systems and infrastructure that support critical functions or processes in the event of a disruption or disaster. DRPs are not in place, as they may affect the availability and continuity of the ICS and its functions or processes in case of a failure or incident. However, this concern may not be related to older unsupported technology, as it may apply to any ICS regardless of its technology level. Technical specifications are not documented is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Technical specifications are documents that describe the technical characteristics or requirements of a system or component, such as functionality, performance, design, etc. Technical specifications are not documented, as they may affect the understanding, maintenance, and improvement of the ICS and its components. However, this concern may not be associated with older unsupported technology, as it may affect any ICS regardless of its technology level.

NEW QUESTION 106
- (Topic 2)
Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at test?

A. Short key length
B. Random key generation
C. Use of symmetric encryption
D. Use of asymmetric encryption

Answer: A

Explanation:
The condition that would be of most concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at rest is short key length. A brute force attack is a method of breaking encryption by trying all possible combinations of keys until finding the correct one. The shorter the key length, the easier it is for an attacker to guess or crack the encryption. Random key generation, use of symmetric encryption, and use of asymmetric encryption are not conditions that would increase the risk of a successful brute force attack. In fact, random key generation can enhance security by preventing predictable patterns in key selection. Symmetric encryption and asymmetric encryption are different types of encryption that have their own advantages and disadvantages, but neither is inherently more vulnerable to brute force attacks than the other. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 107
- (Topic 2)
The performance, risks, and capabilities of an IT infrastructure are BEST measured using a:

A. risk management review
B. control self-assessment (CSA).
C. service level agreement (SLA).
D. balanced scorecard.

Answer: C

Explanation:
A service level agreement (SLA) is a contract between a service provider and a customer that defines the expected level of performance, risks, and capabilities of an IT infrastructure. An IS auditor can use an SLA to measure how well the IT infrastructure meets the business needs and objectives, as well as to identify any gaps or issues that need to be addressed. The other options are not directly related to measuring the performance, risks, and capabilities of an IT infrastructure.
References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.2.11
? CISA Review Questions, Answers & Explanations Database, Question ID 203

NEW QUESTION 108
- (Topic 2)
Which of the following Is the BEST way to ensure payment transaction data is restricted to the appropriate users?

A. Implementing two-factor authentication

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

Answer: C

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

NEW QUESTION 113
- (Topic 2)
Which of the following BEST demonstrates that IT strategy Is aligned with organizational goals and objectives?

A. IT strategies are communicated to all Business stakeholders
B. Organizational strategies are communicated to the chief information officer (CIO).
C. Business stakeholders are Involved In approving the IT strategy.
D. The chief information officer (CIO) is involved In approving the organizational strategies

Answer: C

Explanation:
Business stakeholders being involved in approving the IT strategy best demonstrates that IT strategy is aligned with organizational goals and objectives. IT strategy is a plan that defines how IT resources and capabilities will support and enable the achievement of business goals and objectives. Business stakeholders are the individuals or groups who have an interest or influence in the organization's activities and outcomes. By involving business stakeholders in approving the IT strategy, the organization can ensure that the IT strategy reflects and supports the business needs, expectations, and priorities. The other options do not necessarily indicate that IT strategy is aligned with organizational goals and objectives, as they do not involve the participation or feedback of business stakeholders. References: CISA Review Manual, 27th Edition, page 97

NEW QUESTION 114
- (Topic 2)
Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

A. Findings from prior audits
B. Results of a risk assessment
C. An inventory of personal devices to be connected to the corporate network
D. Policies including BYOD acceptable user statements

Answer: D

Explanation:
The most important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program is policies including BYOD acceptable user statements. Policies are documents that define the organization's objectives, requirements, expectations, and responsibilities regarding a specific topic or area. BYOD policies should include acceptable user statements that specify what types of personal devices are allowed to connect to the corporate network, what security measures must be implemented on those devices, what data can be accessed or stored on those devices, what actions must be taken in case of device loss or theft, and what consequences will apply for non-compliance. Policies including BYOD acceptable user statements can provide an IS auditor with a clear understanding of the scope, criteria, and objectives of the BYOD program audit. Findings from prior audits, results of a risk assessment, and an inventory of personal devices to be connected to the corporate network are also useful inputs for planning a BYOD program audit, but they are not as important as policies including BYOD acceptable user statements. References: ISACA CISA Review Manual 27th Edition, page 381.

NEW QUESTION 115
- (Topic 2)
In an environment that automatically reports all program changes, which of the following is the MOST efficient way to detect unauthorized changes to production programs?

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

Answer: A

Explanation:
Reviewing the last compile date of production programs is the most efficient way to detect unauthorized changes to production programs, as it can quickly identify any discrepancies between the expected and actual dates of program modification. The last compile date is a timestamp that indicates when a program was last compiled or translated from source code to executable code. Any changes to the source code would require a recompilation, which would update the last compile date. The IS auditor can compare the last compile date of production programs with the authorized change requests and reports to verify that only approved changes were implemented. The other options are not as efficient as option A, as they are more time-consuming, labor-intensive or error-prone. Manually comparing code in production programs to controlled copies is a method of verifying that the code in production matches the code in a secure repository or library, but it requires access to both versions of code and a tool or technique to compare them line by line. Periodically running and reviewing test data against production

programs is a method of verifying that the programs produce the expected outputs and results, but it requires designing, executing and evaluating test cases for each program. Verifying user management approval of modifications is a method of verifying that the changes to production programs were authorized and documented, but it does not ensure that the changes were implemented correctly or accurately. References: CISA Review Manual (Digital Version) , Chapter 4: Information Systems Operations and Business Resilience, Section 4.3: Change Management Practices.

NEW QUESTION 119
- (Topic 1)
An IS auditor is examining a front-end subledger and a main ledger. Which of the following would be the GREATEST concern if there are flaws in the mapping of accounts between the two systems?

A. Double-posting of a single journal entry
B. Inability to support new business transactions
C. Unauthorized alteration of account attributes
D. Inaccuracy of financial reporting

Answer: D

Explanation:
The greatest concern for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger is the inaccuracy of financial reporting. A subledger is a detailed record of transactions for a specific account, such as accounts receivable, accounts payable, inventory, or fixed assets. A main ledger is a summary record of all transactions for all accounts in an accounting system. The mapping of accounts between a subledger and a main ledger is the process of linking or reconciling the transactions in the subledger with the corresponding entries in the main ledger. If there are flaws in the mapping of accounts, such as missing, duplicated, or incorrect transactions, the main ledger may not reflect the true financial position and performance of the organization. This may lead to inaccurate financial reporting, which may affect decision making, compliance, auditing, taxation, and stakeholder confidence.
Double-posting of a single journal entry, inability to support new business transactions, and unauthorized alteration of account attributes are not the greatest concerns for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger. These are possible consequences or causes of flaws in the mapping of accounts, but they do not have as significant an impact as inaccuracy of financial reporting. Double- posting of a single journal entry may result in errors or discrepancies in the main ledger balances. Inability to support new business transactions may indicate limitations or inefficiencies in the accounting system design or configuration. Unauthorized alteration of account attributes may suggest weaknesses or breaches in access control or segregation of duties.

NEW QUESTION 124
- (Topic 1)
Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

A. System flowchart
B. Data flow diagram
C. Process flowchart
D. Entity-relationship diagram

Answer: C

Explanation:
The best document for an IS auditor to use in detecting a weakness in segregation of duties is a process flowchart. A process flowchart is a diagram that illustrates the sequence of steps, activities, tasks, or decisions involved in a business process. A process flowchart can help detect a weakness in segregation of duties by showing who performs what actions or roles in a process, and whether there is any overlap or conflict of interest among them. The other options are not as useful as a process flowchart in detecting a weakness in segregation of duties, as they do not show who performs what actions or roles in a process. A system flowchart is a diagram that illustrates the components, functions, interactions, or logic of an information system. A data flow diagram is a diagram that illustrates how data flows from sources to destinations through processes, stores, or external entities. An entity-relationship diagram is a diagram that illustrates how entities (such as tables) are related to each other through attributes (such as keys) in a database. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 127
- (Topic 1)
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

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

Answer: A

Explanation:
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor’s best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet, as this would provide an additional layer of security and alert the organization of any malicious traffic that bypasses or penetrates the firewall. Placing an IDS between the firewall and the demilitarized zone (DMZ), the organization’s web server, or the organization’s network would not be as effective, as it would only monitor the traffic that has already passed through the firewall. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.3

NEW QUESTION 128
- (Topic 1)
An organization has recently acquired and implemented intelligent-agent software for granting loans to customers. During the post-implementation review, which of the following is the MOST important procedure for the IS auditor to perform?

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

D. Review system documentation to ensure completeness.

Answer: B

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

NEW QUESTION 131
- (Topic 1)
During the design phase of a software development project, the PRIMARY responsibility of an IS auditor is to evaluate the:

A. Future compatibility of the application.
B. Proposed functionality of the application.
C. Controls incorporated into the system specifications.
D. Development methodology employed.

Answer: C

Explanation:
The primary responsibility of an IS auditor during the design phase of a software development project is to evaluate the controls incorporated into the system specifications. Controls are mechanisms or procedures that aim to ensure the security, reliability, or performance of a system or process. System specifications are documents that define and describe the requirements, features, functions, or components of a system or software. Evaluating the controls incorporated into the system specifications is a key responsibility of an IS auditor during the design phase of a software development project, as it helps ensure that the system or software meets the organization's objectives, standards, and expectations for security, reliability, or performance. The other options are not primary responsibilities of an IS auditor during the design phase of a software development project, as they do not directly relate to evaluating the controls incorporated into the system specifications. Future compatibility of the application is a possible factor that may affect the functionality or usability of the application in different environments or platforms, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Proposed functionality of the application is a possible factor that may affect the suitability or value of the application for meeting user needs or expectations, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Development methodology employed is a possible factor that may affect the quality or consistency of the software development process, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION 133
- (Topic 1)
Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

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

Answer: C

Explanation:
The greatest concern for an IS auditor reviewing data conversion and migration during the implementation of a new application system is unauthorized data modifications occurred during conversion. Unauthorized data modifications are changes or alterations to data that are not authorized, intended, or expected, such as due to errors, fraud, or sabotage. Unauthorized data modifications occurred during conversion can compromise the accuracy, completeness, and integrity of the data being converted and migrated to the new application system, and may result in data loss, corruption, or inconsistency. The other options are not as concerning as unauthorized data modifications occurred during conversion in reviewing data conversion and migration during the implementation of a new application system, as they do not affect the accuracy, completeness, or integrity of the data being converted and migrated. Data conversion was performed using manual processes is a possible factor that may increase the risk or complexity of data conversion and migration, but it does not necessarily imply that unauthorized data modifications occurred during conversion. Backups of the old system and data are not available online is a possible factor that may affect the availability or accessibility of the old system and data for backup or recovery purposes, but it does not imply that unauthorized data modifications occurred during conversion. The change management process was not formally documented is a possible factor that may affect the quality or consistency of the change management process for implementing the new application system, but it does not imply that unauthorized data modifications occurred during conversion. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION 135
- (Topic 1)
Which of the following is MOST important to include in forensic data collection and preservation procedures?

A. Assuring the physical security of devices
B. Preserving data integrity
C. Maintaining chain of custody
D. Determining tools to be used

Answer: B

Explanation:
The most important thing to include in forensic data collection and preservation procedures is preserving data integrity. Data integrity is the property that ensures that data is accurate, complete, and consistent throughout its lifecycle. Preserving data integrity is essential for forensic data collection and preservation procedures because it ensures that the data can be used as valid and reliable evidence in legal proceedings or investigations. Preserving data integrity can be achieved by using methods such as hashing, checksums, digital signatures, write blockers, tamper-evident seals, or timestamps. The other options are not as important as preserving data integrity in forensic data collection and preservation procedures, as they do not affect the validity or reliability of the data. Assuring the physical security of devices is a security measure that protects devices from unauthorized access, theft, damage, or destruction, but it does not ensure that the

data on the devices is accurate, complete, and consistent. Maintaining chain of custody is a documentation technique that records and tracks the handling and transfer of devices or data among different parties involved in forensic activities, but it does not ensure that the data on the devices is accurate, complete, and consistent. Determining tools to be used is a planning activity that selects and prepares the appropriate tools for forensic data collection and preservation procedures, but it does not ensure that the data collected and preserved by the tools is accurate, complete, and consistent. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION 137
- (Topic 1)
Which of the following fire suppression systems needs to be combined with an automatic switch to shut down the electricity supply in the event of activation?

A. Carbon dioxide
B. FM-200
C. Dry pipe
D. Halon

Answer: A

Explanation:
Carbon dioxide fire suppression systems need to be combined with an automatic switch to shut down the electricity supply in the event of activation. This is because carbon dioxide displaces oxygen in the air and can create a suffocation hazard for people in the protected area. Therefore, it is essential to cut off the power source before releasing carbon dioxide to avoid electrical shocks and sparks that could ignite the fire again. Carbon dioxide systems are typically used for total flooding applications in spaces that are not habitable, such as server rooms or data centers.

NEW QUESTION 142
- (Topic 1)
Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

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

Answer: D

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

NEW QUESTION 147
- (Topic 1)
An IT balanced scorecard is the MOST effective means of monitoring:

A. governance of enterprise IT.
B. control effectiveness.
C. return on investment (ROI).
D. change management effectiveness.

Answer: A

Explanation:
An IT balanced scorecard is a strategic management tool that aligns IT objectives with business goals and measures the performance of IT processes using key performance indicators (KPIs). It is the most effective means of monitoring governance of enterprise IT, which is the process of ensuring that IT supports the organization’s strategy and objectives. Governance of enterprise IT covers aspects such as IT value delivery, IT risk management, IT resource management, and IT performance measurement. An IT balanced scorecard can help monitor these aspects and provide feedback to improve IT governance. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

NEW QUESTION 149
- (Topic 1)
Which of the following is MOST important for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros?

A. Encryption of the spreadsheet
B. Version history
C. Formulas within macros
D. Reconciliation of key calculations

Answer: C

Explanation:
The most important thing for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros is the formulas within macros. Macros are sequences of commands or instructions that can automate tasks or calculations in a spreadsheet. Formulas are expressions that perform calculations on values or data in a spreadsheet. The accuracy of a spreadsheet depends largely on whether the formulas within macros are correct, consistent, and complete. The IS auditor should review the formulas within macros to verify that they produce the expected results and do not contain any errors or inconsistencies. The

other options are not as important as formulas within macros, as they do not directly affect the accuracy of a spreadsheet. Encryption of the spreadsheet is a security control that can protect the confidentiality and integrity of the spreadsheet, but it does not ensure its accuracy. Version history is a document control feature that can track and manage changes to the spreadsheet, but it does not verify its accuracy. Reconciliation of key calculations is a validation technique that can compare and confirm the results of calculations with other sources, but it does not evaluate the accuracy of formulas within macros. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 153
- (Topic 1)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

Explanation:
The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical expressions that define the business requirements and constraints for specific data elements. They can be used to validate, transform, or filter incoming data from external sources, ensuring that only high-quality data is accepted into the enterprise data warehouse. Business rules can also help to identify and resolve data quality issues, such as missing values, duplicates, outliers, or inconsistencies.

NEW QUESTION 158
- (Topic 3)
Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

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

Answer: C

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

NEW QUESTION 163
- (Topic 3)
Which of the following is the BEST reason to implement a data retention policy?

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

Answer: A

Explanation:
The best reason to implement a data retention policy is to limit the liability associated with storing and protecting information. A data retention policy is a document that defines how long data should be kept by an organization and how they should be disposed of when they are no longer needed. A data retention policy should comply with the applicable laws and regulations that govern the data retention requirements and obligations of organizations, such as tax laws, privacy laws, or industry standards4. Implementing a data retention policy can help to limit the liability associated with storing and protecting information by reducing the amount of data that need to be stored and secured, minimizing the risk of data breaches or leaks, ensuring compliance with legal or contractual obligations, and avoiding potential fines or penalties for non- compliance5. The other options are less relevant or incorrect because:
? B. Documenting business objectives for processing data within the organization is not a reason to implement a data retention policy, as it is more related to data governance than data retention. Data governance refers to the policies, procedures, and controls that define how data are collected, used, managed, and shared within an organization. Data governance helps to ensure that data are aligned with business objectives and support decision making6.
? C. Assigning responsibility and ownership for data protection outside IT is not a reason to implement a data retention policy, as it is more related to data accountability than data retention. Data accountability refers to the identification and assignment of roles and responsibilities for data protection among different stakeholders within an organization. Data accountability helps to ensure that data are handled appropriately and securely by authorized parties7.
? D. Establishing a recovery point objective (RPO) for disaster recovery procedures is not a reason to implement a data retention policy, as it is more related to data backup than data retention. Data backup refers to the process of creating copies of data that can be restored in case of data loss or corruption. Data backup helps to ensure that data are available and recoverable in case of disaster8. RPO is a measure of the maximum amount of data that can be lost or acceptable in case of disaster9. References: Data Retention Policy - ISACA, Data Retention - ISACA, Data Governance - ISACA, Data Accountability - ISACA, Data Backup - ISACA, Recovery Point Objective - ISACA

NEW QUESTION 168
- (Topic 3)
Which of the following features of a library control software package would protect against unauthorized updating of source code?

A. Required approvals at each life cycle step
B. Date and time stamping of source and object code

C. Access controls for source libraries
D. Release-to-release comparison of source code

Answer: C

Explanation:
Access controls for source libraries are the features of a library control software package that would protect against unauthorized updating of source code. Access controls are the mechanisms that regulate who can access, modify, or delete the source code stored in the source libraries. Source libraries are the repositories that contain the source code files and their versions. By implementing access controls for source libraries, the library control software package can prevent unauthorized or malicious users from tampering with the source code and compromising its integrity, security, or functionality1. The other options are not as effective as access controls for source libraries in protecting against unauthorized updating of source code. Option A, required approvals at each life cycle step, is a good practice but may not be sufficient to prevent unauthorized updates if the approval process is bypassed or compromised. Option B, date and time stamping of source and object code, is a useful feature but may not prevent unauthorized updates if the date and time stamps are altered or ignored. Option D, release-to-release comparison of source code, is a helpful feature but may not prevent unauthorized updates if the comparison results are not reviewed or acted upon.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? How to protect your source code from attackers2
? How to Stop Unauthorized Use of Open Source Code

NEW QUESTION 171
- (Topic 3)
During an IT general controls audit of a high-risk area where both internal and external audit teams are reviewing the same approach to optimize resources?

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

Answer: A

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

NEW QUESTION 173
- (Topic 3)
Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

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

Answer: D

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

NEW QUESTION 178
- (Topic 3)
in a controlled application development environment, the MOST important segregation of duties should be between the person who implements changes into the production environment and the:

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

Answer: A

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

NEW QUESTION 180
- (Topic 3)
Which of the following backup schemes is the BEST option when storage media is limited?

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

Answer: C

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

NEW QUESTION 183
- (Topic 3)
Which task should an IS auditor complete FIRST during the preliminary planning phase of a database security review?

A. Perform a business impact analysis (BIA).
B. Determine which databases will be in scope.
C. Identify the most critical database controls.
D. Evaluate the types of databases being used

Answer: B

Explanation:
The first task that an IS auditor should complete during the preliminary planning phase of a database security review is to determine which databases will be in scope. The scope defines the boundaries and objectives of the audit, as well as the resources, time, and budget required. The IS auditor should identify the databases that are relevant to the audit based on factors such as their criticality, risk, complexity, size, type, location, and ownership. The IS auditor should also consider the regulatory, contractual, and organizational requirements that apply to the databases. By defining the scope clearly and accurately, the IS auditor can ensure that the audit is focused, feasible, and effective. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 186
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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