Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (Topic 3)
A review of Internet security disclosed that users have individual user accounts with Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only the corporate network is used. The organization should FIRST:

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

Answer: D

Explanation:
The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use. A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data1. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personal accounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.
The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 247
? What is a Security Policy? Definition, Elements, and Examples - Varonis1

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

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

Answer: B

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

NEW QUESTION 3
- (Topic 3)
Which of the following is MOST important for an IS auditor to look for in a project feasibility study?

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

Answer: C

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

NEW QUESTION 4
- (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 5
- (Topic 3)
Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

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

Answer: D

Explanation:
The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources, procedures, communication plans, and backup arrangements3. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements. Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident4. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:
? A. The BCP's contact information needs to be updated is not a great concern for an IS auditor reviewing an organization's BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.
? B. The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization's BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or effectiveness of the BCP.
? C. The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization's BCP, as it is a high-level issue that can be resolved. Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization. Approval by senior management helps to ensure that the BCP is aligned with the organization's strategy, objectives, and priorities, and that it has sufficient resources and authority to be implemented. Approval by senior management also helps to increase the awareness and commitment of the organization's stakeholders to the BCP. While having no approval by senior management may affect the credibility and acceptance of the BCP, it does not affect the overall validity or effectiveness of the BCP. References: Working Toward a Managed, Mature Business Continuity Plan - ISACA, ISACA Introduces New Audit Programs for Business Continuity/Disaster …, Disaster Recovery and Business Continuity Preparedness for Cloud-based …

NEW QUESTION 6
- (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 7
- (Topic 3)

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

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

Answer: B

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

NEW QUESTION 8
- (Topic 3)
What Is the BEST method to determine if IT resource spending is aligned with planned project spending?

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

Answer: A

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

NEW QUESTION 9
- (Topic 3)
An IS auditor finds that the process for removing access for terminated employees is not documented What is the MOST significant risk from this observation?

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

Answer: D

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

NEW QUESTION 10
- (Topic 3)
An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should

be the MAJOR concern with this situation?

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

Answer: C

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

NEW QUESTION 10
- (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 14
- (Topic 3)
Which of the following is MOST critical for the effective implementation of IT governance?

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

Answer: C

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

NEW QUESTION 15
- (Topic 3)
An IS auditor reviewing the threat assessment tor a data center would be MOST concerned if:

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

Answer: C

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

NEW QUESTION 18
- (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 20
- (Topic 3)
Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA> to automate routine business tasks?

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

Answer: A

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

NEW QUESTION 21
- (Topic 3)
An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported the auditee has stated that it will take six

months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

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

Answer: C

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

NEW QUESTION 23
- (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 25
- (Topic 3)
Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

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

Answer: C

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

NEW QUESTION 29
- (Topic 3)
Which of the following BEST describes an audit risk?

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

Answer: B

Explanation:
The best description of an audit risk is that the financial report may contain undetected material errors. Audit risk is the risk that the auditor expresses an inappropriate opinion on the financial report when it contains material misstatements or errors. Audit risk consists of three components: inherent risk, control risk,

and detection risk. Inherent risk is the susceptibility of an assertion or a control to a material misstatement or error due to factors such as complexity, volatility, fraud, or human error. Control risk is the risk that a material misstatement or error will not be prevented or detected by the internal controls. Detection risk is the risk that the auditor's procedures will not detect a material misstatement or error that exists in an assertion or a control. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 33
- (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 37
- (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 39
- (Topic 3)
Which of the following is the PRIMARY advantage of using visualization technology for corporate applications?

A. Improved disaster recovery
B. Better utilization of resources
C. Stronger data security
D. Increased application performance

Answer: B

Explanation:
Visualization technology is the use of software and hardware to create graphical representations of data, such as charts, graphs, maps, images, etc. Visualization technology can help users to understand, analyze, and communicate complex and large amounts of data in an intuitive and engaging way1.
One of the primary advantages of using visualization technology for corporate applications is that it can improve the utilization of resources, such as time, money, human capital, and physical assets. Some of the ways that visualization technology can achieve this are:
? Visualization technology can help users to quickly and easily explore, filter, and interact with data, reducing the need for manual data processing and analysis1. This can save time and effort for both data producers and consumers, and allow them to focus on more value-added tasks.
? Visualization technology can help users to discover patterns, trends, outliers, correlations, and causations in data that may otherwise be hidden or overlooked in traditional reports or tables1. This can enable users to make better and faster decisions based on data-driven insights, and optimize their strategies and actions accordingly.
? Visualization technology can help users to communicate and share data more effectively and persuasively with different audiences, such as customers, partners, investors, regulators, etc1. This can enhance the reputation and credibility of the organization, and foster collaboration and innovation among stakeholders.
? Visualization technology can help users to monitor and measure the performance

and impact of their activities, products, services, or processes1. This can help users to identify problems or opportunities for improvement, and adjust their plans or actions accordingly.
? Visualization technology can help users to create engaging and interactive
experiences for their customers or end-users1. This can increase customer satisfaction and loyalty, and generate more revenue or value for the organization.
Therefore, using visualization technology for corporate applications can help organizations to better utilize their resources and achieve their goals.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? TechRadar Blog, Best data visualization tools of 20232
? IBM Blog, What is Data Visualization?3
? TDWI Blog, Data Visualization Technology4
? Tableau Blog, What are the advantages and disadvantages of data visualization?

NEW QUESTION 41
- (Topic 3)
The PRIMARY role of a control self-assessment (CSA) facilitator is to:

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

Answer: B

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

NEW QUESTION 45
- (Topic 3)
An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in- house. Which of the following findings should be the IS auditor's GREATEST concern?

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

Answer: D

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

NEW QUESTION 47
- (Topic 3)
Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

A. Customer service complaints

B. Automated monitoring of logs
C. Server crashes
D. Penetration testing

Answer: B

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

NEW QUESTION 49
- (Topic 3)
Which of the following would be of GREATEST concern when reviewing an organization's security information and event management (SIEM) solution?

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

Answer: C

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

NEW QUESTION 53
- (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 58
- (Topic 3)
An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which at the following is the BEST recommendation?

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

Answer: A

Explanation:
The best recommendation for improving IT governance within the organization is to implement key performance indicators (KPIs). KPIs are measurable values that show how effectively the organization is achieving its key business objectives. KPIs can help the organization to monitor and evaluate the performance, efficiency, and alignment of its IT processes and resources with its business goals and strategies1.

The other options are not as effective as implementing KPIs for improving IT governance. Option B, implementing annual third-party audits, is a good practice but may not be sufficient or timely to identify and address the issues or gaps in IT governance. Option C, benchmarking organizational performance against industry peers, is a useful technique but may not reflect the specific needs and expectations of the organization’s stakeholders. Option D, requiring executive management to draft IT strategy, is a necessary step but not enough to ensure that IT governance is implemented and monitored throughout the organization.

NEW QUESTION 61
- (Topic 3)
An externally facing system containing sensitive data is configured such that users have either read-only or administrator rights. Most users of the system have administrator access. Which of the following is the GREATEST risk associated with this situation?

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

Answer: C

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

NEW QUESTION 65
- (Topic 2)
An IS auditor is conducting a review of a data center. Which of the following observations could indicate an access control Issue?

A. Security cameras deployed outside main entrance
B. Antistatic mats deployed at the computer room entrance
C. Muddy footprints directly inside the emergency exit
D. Fencing around facility is two meters high

Answer: C

Explanation:
An IS auditor is conducting a review of a data center. An observation that could indicate an access control issue is muddy footprints directly inside the emergency exit. Access control is a process that ensures that only authorized entities or individuals can access or use an information system or resource, and prevents unauthorized access or use. Access control can be implemented using various methods or mechanisms, such as physical, logical, administrative, etc. Muddy footprints directly inside the emergency exit could indicate an access control issue, as they could suggest that someone has entered the data center through the emergency exit without proper authorization or authentication, and potentially compromised the security or integrity of the data center. Security cameras deployed outside main entrance is not an observation that could indicate an access control issue, but rather a control that could enhance access control, as security cameras are devices that capture and record video footage of the surroundings, and can help monitor and deter unauthorized access or activity. Antistatic mats deployed at the computer room entrance is not an observation that could indicate an access control issue, but rather a control that could prevent static electricity damage, as antistatic mats are devices that dissipate or reduce static charges from people or objects, and can help protect electronic equipment from electrostatic discharge (ESD). Fencing around facility is two meters high is not an observation that could indicate an access control issue, but rather a control that could improve physical security, as fencing is a barrier that encloses or surrounds an area, and can help prevent unauthorized entry or intrusion.

NEW QUESTION 70
- (Topic 2)
Which of the following documents should specify roles and responsibilities within an IT audit organization?

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

Answer: B

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

NEW QUESTION 72
- (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 77
- (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 78
- (Topic 2)
The PRIMARY reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?

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

Answer: B

Explanation:
The primary reason for an IS auditor to use data analytics techniques is to reduce detection risk. Detection risk is the risk that an IS auditor will fail to detect material errors or irregularities in the information systems environment. By using data analytics techniques, such as data extraction, analysis, visualization, and reporting, an IS auditor can enhance the audit scope, coverage, efficiency, and effectiveness. Data analytics techniques can help an IS auditor to identify anomalies, patterns, trends, correlations, and outliers in large volumes of data that may indicate potential issues or risks. Technology risk, control risk, and inherent risk are types of audit risk that are not directly affected by the
use of data analytics techniques by an IS auditor. References: [ISACA Journal Article: Data Analytics for Auditors]

NEW QUESTION 81
- (Topic 2)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

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

Answer: C

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

NEW QUESTION 83
- (Topic 2)
The PRIMARY focus of a post-implementation review is to verify that:

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

Answer: B

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

NEW QUESTION 88
- (Topic 2)
The waterfall life cycle model of software development is BEST suited for which of the following situations?

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

Answer: A

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

NEW QUESTION 89
- (Topic 2)
While auditing a small organization's data classification processes and procedures, an IS auditor noticed that data is often classified at the incorrect level. What is the MOST effective way for the organization to improve this situation?

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

Answer: B

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

NEW QUESTION 93
- (Topic 2)
Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

A. The job scheduler application has not been designed to display pop-up error messages.
B. Access to the job scheduler application has not been restricted to a maximum of two staff members

C. Operations shift turnover logs are not utilized to coordinate and control the processing environment
D. Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor

Answer: D

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

NEW QUESTION 96
- (Topic 2)
When auditing the alignment of IT to the business strategy, it is MOST Important for the IS auditor to:

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

Answer: D

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

NEW QUESTION 101
- (Topic 2)
Which of the following is MOST important to consider when scheduling follow-up audits?

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

Answer: B

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

NEW QUESTION 106
- (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 109
- (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 112
- (Topic 2)
A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed Which of the following is the MOST important requirement to include In the vendor contract to ensure continuity?

A. Continuous 24/7 support must be available.
B. The vendor must have a documented disaster recovery plan (DRP) in place.
C. Source code for the software must be placed in escrow.
D. The vendor must train the organization's staff to manage the new software

Answer: C

Explanation:
Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.51
? CISA Review Questions, Answers & Explanations Database, Question ID 228

NEW QUESTION 115
- (Topic 2)
Which of the following is a social engineering attack method?

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

Answer: A

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

NEW QUESTION 120
- (Topic 2)
Which of the following BEST enables the timely identification of risk exposure?

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

Answer: C

Explanation:
Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk

exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References:
ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION 121
- (Topic 2)
An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

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

Answer: C

Explanation:
This should be the IS auditor’s greatest concern, because it means that the organization has not considered the potential impact of the cloud document storage solution on its ability to continue its operations in the event of a disruption or disaster. A BCP is a document that outlines the procedures and actions to be taken in order to maintain or resume critical business functions during and after a crisis. A BCP should be updated whenever there is a significant change in the organization’s IT infrastructure, systems, processes, or dependencies, such as implementing a cloud document storage solution. The IS auditor should verify that the BCP reflects the current state of the organization’s IT environment, and that it addresses the risks, challenges, and opportunities associated with the cloud document storage solution.
The other options are not as concerning as the BCP not being updated:
? Users are not required to sign updated acceptable use agreements. This is a minor concern, but it does not pose a major threat to the organization’s business continuity. Acceptable use agreements are documents that define the rules and guidelines for using IT resources, such as the cloud document storage solution. Users should sign updated acceptable use agreements to acknowledge their responsibilities and obligations, and to comply with the organization’s policies and standards. However, this does not affect the organization’s ability to continue its operations in a crisis.
? Users have not been trained on the new system. This is a moderate concern, but it does not jeopardize the organization’s business continuity. Training users on the new system is important to ensure that they can use it effectively and efficiently, and to avoid errors or misuse that could compromise the security or performance of the system. However, this does not prevent the organization from accessing or restoring its data in a crisis.
? Mobile devices are not encrypted. This is a serious concern, but it does not directly impact the organization’s business continuity. Encrypting mobile devices is a security measure that protects the data stored on them from unauthorized access or disclosure in case of loss or theft. However, this does not affect the availability or integrity of the data stored in the cloud document storage solution, which should have its own encryption mechanisms.

NEW QUESTION 126
- (Topic 2)
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

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

Answer: B

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

NEW QUESTION 131
- (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 136
- (Topic 2)

Which of the following is the PRIMARY reason to follow a configuration management process to maintain application?

A. To optimize system resources
B. To follow system hardening standards
C. To optimize asset management workflows
D. To ensure proper change control

Answer: D

Explanation:
Following a configuration management process to maintain applications is the primary reason for ensuring proper change control. Configuration management is a process of identifying, documenting, controlling, and verifying the configuration items and their interrelationships within an IT system or environment. Following a configuration management process can help to ensure that any changes to the applications are authorized, tested, documented, and tracked throughout their lifecycle. This will help to prevent unauthorized or improper changes that could affect the functionality, performance, or security of the applications. The other options are not the primary reasons for following a configuration management process, but rather possible benefits or outcomes of doing so. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
? CISA Review Questions, Answers & Explanations Database, Question ID 225

NEW QUESTION 141
- (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 143
- (Topic 2)
Which of the following is the MAIN purpose of an information security management system?

A. To identify and eliminate the root causes of information security incidents
B. To enhance the impact of reports used to monitor information security incidents
C. To keep information security policies and procedures up-to-date
D. To reduce the frequency and impact of information security incidents

Answer: D

Explanation:
The main purpose of an information security management system (ISMS) is to reduce the frequency and impact of information security incidents. An ISMS is a systematic approach to managing information security risks, policies, procedures, and controls within an organization. An ISMS aims to ensure the confidentiality, integrity, and availability of information assets, as well as to comply with relevant laws and regulations. The other options are not the main purpose of an ISMS, but rather some of its possible benefits or components. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.11
? CISA Review Questions, Answers & Explanations Database, Question ID 205

NEW QUESTION 145
- (Topic 2)
Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor's BEST recommendation for a compensating control?

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

Answer: A

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

prevent unauthorized, duplicate or erroneous payments from being processed by the accounts payable system. Reviewing payment transaction history is a control that monitors and analyzes the payment transactions after they have been processed by the accounts payable system, but it does not prevent unauthorized, duplicate
or erroneous payments from occurring in the first place. References: CISA Review Manual
(Digital Version) , Chapter 5: Protection of Information Assets, Section 5.2: Logical Access.

NEW QUESTION 146
- (Topic 2)
What is the MAIN reason to use incremental backups?

A. To improve key availability metrics
B. To reduce costs associates with backups
C. To increase backup resiliency and redundancy
D. To minimize the backup time and resources

Answer: D

Explanation:
Incremental backups are backups that only copy the data that has changed since the last backup, whether it was a full or incremental backup. The main reason to use incremental backups is to minimize the backup time and resources, as they require less storage space and network bandwidth than full backups. Incremental backups can also improve key availability metrics, such as recovery point objective (RPO) and recovery time objective (RTO), but that is not their primary purpose. Reducing costs associated with backups and increasing backup resiliency and redundancy are possible benefits of incremental backups, but they depend on other factors, such as the backup frequency, retention policy, and media type. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION 151
- (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 152
- (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 157
- (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 159
- (Topic 2)
An information systems security officer's PRIMARY responsibility for business process applications is to:

A. authorize secured emergency access
B. approve the organization's security policy
C. ensure access rules agree with policies
D. create role-based rules for each business process

Answer: C

Explanation:
Ensuring access rules agree with policies is an information systems security officer’s primary responsibility for business process applications. An information systems security officer should verify that the access controls implemented for the business process applications are consistent with the organization’s security policy and objectives. The other options are not the primary responsibility of an information systems security officer, but rather the tasks of an application owner, a senior management, or a business analyst. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.3.11
? CISA Review Questions, Answers & Explanations Database, Question ID 208

NEW QUESTION 163
- (Topic 2)
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control sell-assessment (CSA)?

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

Answer: D

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

NEW QUESTION 165
- (Topic 2)
Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simu-lation test administered for staff members?

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

Answer: A

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

NEW QUESTION 168
- (Topic 2)
An organization is planning an acquisition and has engaged an IS auditor lo evaluate the IT governance framework of the target company. Which of the following would be MOST helpful In determining the effectiveness of the framework?

A. Sell-assessment reports of IT capability and maturity
B. IT performance benchmarking reports with competitors
C. Recent third-party IS audit reports
D. Current and previous internal IS audit reports

Answer: C

Explanation:
Recent third-party IS audit reports would be most helpful in determining the effectiveness of the IT governance framework of the target company. IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. A third-party IS audit is an independent and objective examination of an organization's IT governance framework by an external auditor. Recent third-party IS audit reports can provide reliable and unbiased evidence of the strengths, weaknesses, and maturity of the IT governance framework of the target company. The other options are not as helpful as recent third-party IS audit reports, as they may not be as comprehensive, accurate, or current as external audits. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION 169
- (Topic 2)
Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

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

Answer: D

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

NEW QUESTION 174
- (Topic 2)
The IS auditor has recommended that management test a new system before using it in production mode. The BEST approach for management in developing a test plan is to use processing parameters that are:

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

Answer: D

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

NEW QUESTION 179
- (Topic 2)
Capacity management enables organizations to:

A. forecast technology trends
B. establish the capacity of network communication links
C. identify the extent to which components need to be upgraded
D. determine business transaction volumes.

Answer: C

Explanation:
Capacity management is a process that ensures that the IT resources of an organization are sufficient to meet the current and future demands of the business. Capacity management enables organizations to identify the extent to which components need to be upgraded, by monitoring and analyzing the performance, utilization, and availability of the IT components, such as servers, networks, storage, applications, etc., and identifying any bottlenecks, gaps, or risks that may affect the service level agreements (SLAs) or quality of service (QoS). Capacity management also helps organizations to plan and optimize the use of IT resources, by forecasting the future demand and growth of the business, and aligning the IT capacity with the business needs and objectives. Forecasting technology trends is a possible outcome of capacity management, but it is not its main purpose. Establishing the capacity of network communication links is a part of capacity management, but it is not its main goal. Determining business transaction volumes is an input for capacity management, but it is not its main objective.

NEW QUESTION 184
- (Topic 2)
In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

A. Discovery
B. Attacks
C. Planning
D. Reporting

Answer: A

Explanation:
Penetration testing is a method of evaluating the security of a system or network by simulating an attack from a malicious source. Penetration testing typically consists of four phases: planning, discovery, attacks, and reporting. In the discovery phase, penetration testers gather information about the target system or network, such as host detection, domain name system (DNS) interrogation, port scanning, service identification, operating system fingerprinting, vulnerability scanning, etc. This information can help to identify potential entry points, weaknesses, or vulnerabilities that can be exploited in the subsequent attack phase. Host detection and DNS interrogation are techniques that can be used in the discovery phase to determine the active hosts and their IP addresses and hostnames on the target network. References: [ISACA CISA Review Manual 27th Edition], page 368.

NEW QUESTION 186
- (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 188
- (Topic 2)
Upon completion of audit work, an IS auditor should:

A. provide a report to senior management prior to discussion with the auditee.
B. distribute a summary of general findings to the members of the auditing team.
C. provide a report to the auditee stating the initial findings.
D. review the working papers with the auditee.

Answer: B

Explanation:
Upon completion of audit work, an IS auditor should distribute a summary of general findings to the members of the auditing team. This is to ensure that the audit team members are aware of the audit results, have an opportunity to provide feedback, and can agree on the audit conclusions and recommendations. Providing a report to senior management prior to discussion with the auditee, providing a report to the auditee stating the initial findings, and reviewing the working papers with the auditee are not appropriate actions for an IS auditor to take upon completion of audit work, as they may compromise
the audit independence, objectivity, and quality. References: ISACA CISA Review Manual 27th Edition, page 221

NEW QUESTION 190
- (Topic 2)
Which of the following would MOST effectively ensure the integrity of data transmitted over a network?

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

Answer: D

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

NEW QUESTION 193
- (Topic 2)
After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

A. Verifying that access privileges have been reviewed
B. investigating access rights for expiration dates
C. Updating the continuity plan for critical resources
D. Updating the security policy

Answer: A

Explanation:
The most important task for an IS auditor to perform after the merger of two organizations is to verify that access privileges have been reviewed. Access privileges are the permissions granted to users, groups, or roles to access, modify, or manage IT resources, such as systems, applications, data, or networks. After a merger, the IS auditor should ensure that the access privileges of both organizations are aligned with the new business objectives, policies, and processes, and that there are no conflicts, overlaps, or gaps in the access rights. The IS auditor should also verify that the access privileges are based on the principle of least privilege, which means that users are granted only the minimum level of access required to perform their tasks.
The other options are not as important as verifying that access privileges have been reviewed:
? Investigating access rights for expiration dates is a useful task, but it is not the most important one. Expiration dates are the dates when access rights are automatically revoked or suspended after a certain period of time or after a specific event. The IS auditor should check that the expiration dates are set appropriately and enforced consistently, but this is not as critical as reviewing the access privileges themselves.
? Updating the continuity plan for critical resources is a necessary task, but it is not the most urgent one. A continuity plan is a document that outlines the procedures and actions to be taken in the event of a disruption or disaster that affects the availability of IT resources. The IS auditor should update the continuity plan to reflect the changes and dependencies introduced by the merger, but this can be done after verifying that the access privileges are secure and compliant.
? Updating the security policy is an essential task, but it is not the most immediate one. A security policy is a document that defines the rules and guidelines for securing IT resources and protecting information assets. The IS auditor should update the security policy to incorporate the best practices and standards of both organizations, and to address any new risks or threats posed by the merger, but this can be done after verifying that the access privileges are aligned with the policy.

NEW QUESTION 197
- (Topic 2)
During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements Which of the following is the BEST way to obtain this assurance?

A. Review sign-off documentation
B. Review the source code related to the calculation
C. Re-perform the calculation with audit software
D. Inspect user acceptance lest (UAT) results

Answer: C

Explanation:
The best way to obtain assurance that certain automated calculations comply with the regulatory requirements is to re-perform the calculation with audit software. This will allow the auditor to independently verify the accuracy and validity of the calculation and compare it with the expected results. Reviewing sign-off documentation, source code, or user acceptance test results may not provide sufficient evidence or assurance that the calculation is correct and compliant.
References:
? CISA Review Manual (Digital Version), page 325
? CISA Questions, Answers & Explanations Database, question ID 3335

NEW QUESTION 199
- (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 201
......