Exam Questions CISA

Isaca CISA

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

NEW QUESTION 1
- (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should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective.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 While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.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 2
- (Topic 3)
Which of the following would be an appropriate role of internal audit in helping to establish an organization’s privacy program?

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

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 4
- (Topic 3)
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?

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

Answer: A

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

NEW QUESTION 5
- (Topic 3)
An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

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

Answer: B

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

NEW QUESTION 6
- (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 7
- (Topic 3)
An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

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

Answer: B

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

NEW QUESTION 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)
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 10
- (Topic 3)
In response to an audit finding regarding a payroll application, management implemented a new automated control. Which of the following would be MOST helpful to the IS auditor when evaluating the effectiveness of the new control?

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

Answer: B

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

NEW QUESTION 14
- (Topic 3)
An organization allows its employees lo use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

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

Answer: B

Explanation:
Partitioning the work environment from personal space on devices. This would best maintain information security without compromising employee privacy by

creating a separate and secure area on the personal mobile devices for work-related data and applications. This way, the organization can protect its information from unauthorized access, loss, or leakage, while respecting the employees' personal data and preferences on their own devices.
The other options are not as effective as option B in balancing information security and employee privacy. Option A, installing security software on the devices, is a good practice but may not be sufficient to prevent data breaches or comply with regulatory requirements. Option C, preventing users from adding applications, is too restrictive and may interfere with the employees' personal use of their devices. Option D, restricting the use of devices for personal purposes during working hours, is impractical and difficult to enforce. References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Personal Cellphone Privacy at Work1
? Protecting your personal information and privacy on a company phone2
? Mobile Devices and Protected Health Information (PHI)3
? Using your personal phone for work? Here's how to separate your apps and data4
? 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

NEW QUESTION 16
- (Topic 3)
During a security audit, an IS auditor is tasked with reviewing log entries obtained from an enterprise intrusion prevention system (IPS). Which type of risk would be associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration?

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

Answer: B

Explanation:
The type of risk associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration is detection risk. Detection risk is the risk that the auditor's procedures will not detect a material misstatement or error that exists in an assertion or a control. Detection risk can be affected by factors such as the nature, timing, and extent of the audit procedures, the quality and sufficiency of the audit evidence, and the auditor's professional judgment and competence. Detection risk can be reduced by applying appropriate audit techniques, such as sampling, testing, observation, inquiry, and analysis. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 21
- (Topic 3)
What is the PRIMARY purpose of documenting audit objectives when preparing for an engagement?

A. To address the overall risk associated with the activity under review
B. To identify areas with relatively high probability of material problems
C. To help ensure maximum use of audit resources during the engagement
D. To help prioritize and schedule auditee meetings

Answer: B

Explanation:
The primary purpose of documenting audit objectives when preparing for an engagement is to identify areas with relatively high probability of material problems. Audit objectives are statements that describe what the audit intends to accomplish or verify during the engagement. Audit objectives help the IS auditor to focus on the key areas of risk or concern, to design appropriate audit procedures and tests, and to evaluate audit evidence and results. By documenting audit objectives, the IS auditor can identify areas with relatively high probability of material problems that may affect the achievement of audit goals or business objectives. Addressing the overall risk associated with the activity under review, ensuring maximum use of audit resources during the engagement and prioritizing and scheduling auditee meetings are also purposes of documenting audit objectives, but they are not as primary as identifying areas with high probability of material problems. References:
? CISA Review Manual, 27th Edition, page 1111
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 22
- (Topic 3)
Which of the following presents the GREATEST challenge to the alignment of business and IT?

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

Answer: A

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

NEW QUESTION 27

- (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 31
- (Topic 3)
Which of the following is the BEST way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC)?

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

Answer: B

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

NEW QUESTION 34
- (Topic 3)
Which of the following is the BEST way to enforce the principle of least privilege on a server containing data with different security classifications?

A. Limiting access to the data files based on frequency of use
B. Obtaining formal agreement by users to comply with the data classification policy
C. Applying access controls determined by the data owner
D. Using scripted access control lists to prevent unauthorized access to the server

Answer: C

Explanation:
The best way to enforce the principle of least privilege on a server containing data with different security classifications is to apply access controls determined by the data owner. The principle of least privilege states that users should only have the minimum level of access required to perform their tasks. The data owner is the person who has the authority and responsibility to classify, label, and protect the data according to its sensitivity and value. The data owner can define the access rights and permissions for each user or role based on the data classification policy and the business needs. This will ensure that only authorized and appropriate users can access the data and prevent unauthorized or excessive access that could compromise the confidentiality, integrity, or availability of the data.
References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

NEW QUESTION 36
- (Topic 3)
Which of the following would be MOST useful when analyzing computer performance?

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

Answer: A

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

it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.

The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.

References:

? What is Computer Performance?

? How to Measure Computer Performance

NEW QUESTION 41

- (Topic 3)

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Apply single sign-on for access control

B. Implement segregation of duties.

C. Enforce an internal data access policy.

D. Enforce the use of digital signatures.

Answer: C

Explanation:

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

? CISA Review Manual, 27th Edition, page 2301

? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

NEW QUESTION 46

- (Topic 3)

Which of the following would BEST help to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software?

A. Assign the security risk analysis to a specially trained member of the project management office.

B. Deploy changes in a controlled environment and observe for security defects.

C. Include a mandatory step to analyze the security impact when making changes.

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

Answer: C

Explanation:

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

References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.5

NEW QUESTION 51

- (Topic 3)

A review of an organization’s IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

A. A formal request for proposal (RFP) process

B. Business case development procedures

C. An information asset acquisition policy

D. Asset life cycle management.

Answer: D

Explanation:

Asset life cycle management is a technique of asset management where facility managers maximize the usable life of assets through planning, purchasing, using, maintaining, and disposing of assets1. The main aim of asset life cycle management is to reduce costs and increase productivity by optimizing the performance, reliability, and lifespan of assets2. Asset life cycle management can help prevent the situation of having unused applications by ensuring that the applications are aligned with the business needs, objectives, and strategies, and that they are regularly reviewed, updated, or retired as necessary3.

The other options are not as effective as asset life cycle management for preventing unused applications. A formal request for proposal (RFP) process is a method of soliciting bids from potential vendors or suppliers for a project or service. A RFP process can help select the best application for a specific requirement, but it does not ensure that the application will be used or maintained throughout its lifecycle. Business case development procedures are a set of steps that involve defining the problem, analyzing the alternatives, and proposing a solution for a project or initiative. Business case development procedures can help justify the need and value of an application, but they do not guarantee that the application will be utilized or supported after its implementation. An information asset acquisition policy is a document that outlines the rules and standards for acquiring information assets such as applications. An information asset acquisition policy can help ensure that the applications are acquired in a consistent and compliant manner, but it does not address how the applications will be managed or disposed of after their acquisition.

NEW QUESTION 53

- (Topic 3)

Which of the following is MOST important when planning a network audit?

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

Answer: D

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

NEW QUESTION 54
- (Topic 3)
Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

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

Answer: B

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

NEW QUESTION 59
- (Topic 2)
What is the Most critical finding when reviewing an organization’s information security management?

A. No dedicated security officer
B. No official charier for the information security management system
C. No periodic assessments to identify threats and vulnerabilities
D. No employee awareness training and education program

Answer: C

Explanation:
The most critical finding when reviewing an organization’s information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization’s information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and may not be able to take appropriate measures to mitigate or prevent potential security incidents. No dedicated security officer, no official charter for the information security management system, and no employee awareness training and education program are also findings that may indicate some deficiencies in the organization’s information security management, but they are not as critical as no periodic assessments to identify threats and vulnerabilities. References: ISACA CISA Review Manual 27th Edition, page 343.

NEW QUESTION 64
- (Topic 2)
Due to a recent business divestiture, an organization has limited IT resources to deliver critical projects Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

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

Answer: B

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

NEW QUESTION 65
- (Topic 2)
Which of the following is the BEST reason for an organization to use clustering?

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

Answer: D

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

NEW QUESTION 68
- (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 73
- (Topic 2)
An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

A. There are conflicting permit and deny rules for the IT group.
B. The network security group can change network address translation (NAT).
C. Individual permissions are overriding group permissions.
D. There is only one rule per group with access privileges.

Answer: C

Explanation:
This should result in a finding because it violates the best practice of setting rules for groups rather than users. According to one of the web search results1, using group permissions instead of individual permissions can simplify the management and maintenance of ACLs, reduce the risk of human errors, and ensure consistency and compliance. Individual permissions can create conflicts, confusion, and security gaps in the ACLs. Therefore, the IS auditor should report this as a finding and recommend using group permissions instead.

NEW QUESTION 75
- (Topic 2)
An organization has assigned two now IS auditors to audit a now system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which ol the following is MOST important to meet the IS audit standard for proficiency?

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

Answer: C

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

independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

NEW QUESTION 80
- (Topic 2)
Which of the following would be an appropriate rote of internal audit in helping to establish an organization's privacy program?

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

Answer: A

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

NEW QUESTION 85
- (Topic 2)
Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

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

Answer: A

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

NEW QUESTION 89
- (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 91
- (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 93
- (Topic 2)
Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

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

Answer: C

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

NEW QUESTION 97
- (Topic 2)
Which of the following is the BEST audit procedure to determine whether a firewall is configured in compliance with the organization's security policy?

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

Answer: A

Explanation:
The best audit procedure to determine whether a firewall is configured in compliance with the organization's security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter settings of a firewall, an IS auditor can verify whether they match with the organization's security policy, which is a document that outlines the security objectives, requirements, and guidelines for an organization's information systems and resources. Reviewing the system log is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a system log records events or activities that occur on a firewall, such as connections, requests, responses, errors, alerts, etc., and may not indicate whether they comply with the organization's security policy. Interviewing the firewall administrator is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a firewall administrator may not provide accurate or reliable information about the firewall configuration, and may have conflicts of interest or ulterior motives. Reviewing the actual procedures is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as actual procedures describe how a firewall is configured and maintained, such as installation, testing, updating, etc., and may not reflect whether they comply with the organization's security policy.

NEW QUESTION 101
- (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 106
- (Topic 2)
A project team has decided to switch to an agile approach to develop a replacement for an existing business application. Which of the following should an IS auditor do FIRST to ensure the effectiveness of the protect audit?

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

Answer: C

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

NEW QUESTION 110
- (Topic 2)
Which of the following environments is BEST used for copying data and transformation into a compatible data warehouse format?

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

Answer: C

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

NEW QUESTION 115
- (Topic 2)
An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

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

Answer: D

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

NEW QUESTION 116
- (Topic 2)
Which of the following is MOST helpful for measuring benefits realization for a new system?

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

Answer: C

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

NEW QUESTION 119
- (Topic 2)
Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS audit has been asked to conduct a control assessment. the auditor's BEST course of action would be to determine if:

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

Answer: B

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

NEW QUESTION 121
- (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 124
- (Topic 2)
Which of the following occurs during the issues management process for a system development project?

A. Contingency planning
B. Configuration management
C. Help desk management
D. Impact assessment

Answer: D

Explanation:
Impact assessment is an activity that occurs during the issues management process for a system development project. Issues management is a process of identifying, analyzing, resolving, and monitoring issues that may affect the project scope, schedule, budget, or quality. Impact assessment is a technique of evaluating the severity and priority of an issue, as well as its implications for the project objectives and deliverables. The other options are not activities that occur during the issues management process, but rather related to other processes such as contingency planning, configuration management, or help desk management. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
? CISA Review Questions, Answers & Explanations Database, Question ID 217

NEW QUESTION 128
- (Topic 2)
A third-party consultant is managing the replacement of an accounting system. Which of the following should be the IS auditor's GREATEST concern?

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

Answer: C

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

NEW QUESTION 131
- (Topic 2)
An employee loses a mobile device resulting in loss of sensitive corporate data. Which o(the following would have BEST prevented data leakage?

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

Answer: A

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

NEW QUESTION 135
- (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 137
- (Topic 2)
Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

A. Use of stateful firewalls with default configuration
B. Ad hoc monitoring of firewall activity
C. Misconfiguration of the firewall rules
D. Potential back doors to the firewall software

Answer: C

NEW QUESTION 142
- (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 143
- (Topic 2)
Which of the following is a detective control?

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

Answer: D

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

NEW QUESTION 145
- (Topic 2)
Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?

A. Water sprinkler
B. Fire extinguishers
C. Carbon dioxide (CO2)
D. Dry pipe

Answer: C

Explanation:
The most appropriate and effective fire suppression method for an un-staffed computer room is carbon dioxide (CO2). Carbon dioxide is a gaseous clean agent that extinguishes fire by displacing oxygen and reducing the combustion process. Carbon dioxide is suitable for un-staffed computer rooms because it does not leave any residue, damage, or corrosion on the electronic equipment, and it does not require water or other chemicals that could harm the environment or human health. However, carbon dioxide can pose a risk of asphyxiation to any person who may enter the computer room during or after the discharge, so proper safety precautions and warning signs should be in place.
The other options are not as appropriate or effective as carbon dioxide for an un-staffed computer room:
? Water sprinkler. This is a common fire suppression method that uses water to cool down and extinguish fire. However, water sprinkler is not suitable for un-staffed computer rooms because it can cause severe damage to the electronic equipment, such as short circuits, corrosion, or data loss. Water sprinkler can also create a risk of electric shock to any person who may enter the computer room during or after the discharge.
? Fire extinguishers. These are portable devices that contain a pressurized agent that can be sprayed on a fire to put it out. However, fire extinguishers are not effective for un-staffed computer rooms because they require manual operation by a trained person who can identify the type and location of the fire, and use the appropriate extinguisher. Fire extinguishers can also cause damage to the electronic equipment if they contain water or chemical agents.
? Dry pipe. This is a type of sprinkler system that uses pressurized air or nitrogen in the pipes instead of water until a fire is detected. When a fire is detected, the air or nitrogen is released and water flows into the pipes and sprinklers. However, dry pipe is not ideal for un-staffed computer rooms because it still uses water as the extinguishing agent, which can damage the electronic equipment as mentioned above. Dry pipe also has a slower response time than wet pipe sprinkler systems, which can allow the fire to spread more quickly.

NEW QUESTION 148
- (Topic 2)
Which of the following provides the MOST assurance over the completeness and accuracy ol loan application processing with respect to the implementation of a new system?

A. Comparing code between old and new systems
B. Running historical transactions through the new system

C. Reviewing quality assurance (QA) procedures
D. Loading balance and transaction data to the new system

Answer: B

Explanation:
The most assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system can be obtained by running historical transactions through the new system. Historical transactions are transactions that have been processed and recorded by the old system in the past. Running historical transactions through the new system can provide the most assurance over the completeness and accuracy of loan application processing, by comparing the results and outputs of the new system with those of the old system, and verifying whether they match or differ. This can help identify and resolve any errors or issues that may arise from the new system, such as data conversion, functionality, compatibility, etc. Comparing code between old and new systems is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Code is a set of instructions or commands that define how a system operates or functions. Comparing code between old and new systems can provide some assurance over the completeness and accuracy of loan application processing, by checking whether the logic, algorithms, or functions of the new system are consistent or equivalent with those of the old system. However, this may not be sufficient or reliable, as code may not reflect the actual performance or outcomes of the system, and may not detect any errors or issues that may occur at the data or user level. Reviewing quality assurance (QA) procedures is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. QA procedures are steps or activities that ensure that a system meets its quality standards and requirements, such as testing, verification, validation, etc. Reviewing QA procedures can provide some assurance over the completeness and accuracy of loan application processing, by evaluating whether the new system has been properly tested and verified before implementation. However, this may not be adequate or accurate, as QA procedures may not cover all aspects or scenarios of loan application processing, and may not reveal any errors or issues that may arise after implementation. Loading balance and transaction data to the new system is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Balance and transaction data are data that reflect the status and history of loan applications in a system, such as amounts, dates, payments, etc. Loading balance and transaction data to the new system can provide some assurance over the completeness and accuracy of loan application processing, by transferring data from the old system to the new system and ensuring that they are consistent and correct. However, this may not be enough or valid, as balance and transaction data may not represent all aspects or features of loan application processing, and may not indicate any errors or issues that may arise

NEW QUESTION 150
- (Topic 2)
An IS auditor is reviewing the release management process for an in-house software development solution. In which environment Is the software version MOST likely to be the same as production?

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

Answer: A

Explanation:
A staging environment is a replica of the production environment that is used to test and verify software before deploying it to production. A staging environment is most likely to have the same software version as production, as it mimics the real-world conditions and configurations that will be encountered in production. A testing environment is a separate environment that is used to perform various types of testing on software, such as functional testing, performance testing, security testing, etc. A testing environment may not have the same software version as production, as it may undergo frequent changes or updates based on testing results or feedback. An integration environment is a separate environment that is used to combine and test software components or modules from different developers or sources, to ensure that they work together as expected. An integration environment may not have the same software version as production, as it may involve different versions or branches of software from different sources. A development environment is a separate environment that is used by developers to create and modify software code. A development environment may not have the same software version as production, as it may contain unfinished or untested code that has not been released yet.

NEW QUESTION 155
- (Topic 2)
Which of the following controls BEST ensures appropriate segregation of dudes within an accounts payable department?

A. Ensuring that audit trails exist for transactions
B. Restricting access to update programs to accounts payable staff only
C. Including the creator's user ID as a field in every transaction record created
D. Restricting program functionality according to user security profiles

Answer: D

Explanation:
Restricting program functionality according to user security profiles is the best control for ensuring appropriate segregation of duties within an accounts payable department. An IS auditor should verify that the access rights and permissions of the accounts payable staff are based on their roles and responsibilities, and that they are not able to perform incompatible or conflicting functions such as creating, approving, or paying invoices. This will help to prevent fraud, errors, or abuse of authority within the accounts payable process. The other options are less effective controls for ensuring segregation of duties, as they may involve audit trails, access restrictions, or user identification. References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.31
? CISA Review Questions, Answers & Explanations Database, Question ID 223

NEW QUESTION 158
- (Topic 2)
Which of the following types of firewalls provide the GREATEST degree of control against hacker intrusion?

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

Answer: B

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

NEW QUESTION 161
- (Topic 2)
Which of the following provides IS audit professionals with the BEST source of direction for performing audit functions?

A. Audit charter
B. IT steering committee
C. Information security policy
D. Audit best practices

Answer: A

Explanation:
The audit charter is the document that defines the purpose, authority and responsibility of the IS audit function. It provides IS audit professionals with the best source of direction for performing audit functions, as it establishes the scope, objectives, reporting lines, independence, accountability and resources of the IS audit function. The IT steering committee is a governance body that oversees the strategic alignment, prioritization and direction of IT initiatives, but it does not provide specific guidance for IS audit functions. The information security policy is a document that defines the rules and principles for protecting information assets in the organization, but it does not cover all aspects of IS audit functions. Audit best practices are general guidelines and recommendations for conducting effective and efficient audits, but they are not binding or authoritative sources of direction for IS audit functions. References: CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.1: Audit Charter.

NEW QUESTION 163
- (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 165
- (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 166
- (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 170
- (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 175
- (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 177
- (Topic 2)

Which of the following would BEST help lo support an auditor's conclusion about the effectiveness of an implemented data classification program?

A. Purchase of information management tools
B. Business use cases and scenarios
C. Access rights provisioned according to scheme
D. Detailed data classification scheme

Answer: C

Explanation:
Access rights provisioned according to scheme would best help to support an auditor's conclusion about the effectiveness of an implemented data classification program. This would indicate that the data classification program has been properly implemented and enforced, and that the data is protected according to its sensitivity and value. The other options are not sufficient to demonstrate the effectiveness of a data classification program, as they do not show how the data is actually accessed and used by authorized users. References:
? CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 2042

NEW QUESTION 182
- (Topic 2)
Which of the following MUST be completed as part of the annual audit planning process?

A. Business impact analysis (BIA)
B. Fieldwork
C. Risk assessment
D. Risk control matrix

Answer: C

Explanation:
Risk assessment is a mandatory part of the annual audit planning process, as it helps to identify and prioritize the areas that pose the highest risk to the organization's objectives and operations. Risk assessment involves analyzing the internal and external factors that affect the organization's risk profile, evaluating the likelihood and impact of potential events or scenarios, assessing the existing controls and mitigation strategies, and determining the residual risk level. Based on the risk assessment results, the IS auditor can allocate resources and schedule audits accordingly. A business impact analysis (BIA) is a process that identifies and evaluates the critical business functions and processes that could be disrupted by a disaster or incident, and estimates the potential impact on the organization's operations, reputation and finances. A BIA is not a mandatory part of the annual audit planning process, but it can be used as an input for risk assessment or as a subject for audit. Fieldwork is the phase of an audit where the IS auditor collects evidence to support the audit objectives and conclusions. Fieldwork is not part of the annual audit planning process, but it is part of each individual audit engagement. A risk control matrix is a tool that maps the risks identified in a risk assessment to the controls that mitigate them. A risk control matrix is not a mandatory part of the annual audit planning process, but it can be used as an output of risk assessment or as a tool for audit testing. References:
CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.2: Audit Planning.

NEW QUESTION 186
- (Topic 2)
Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems (lDS)?

A. An increase in the number of identified false positives
B. An increase in the number of detected Incidents not previously identified
C. An increase in the number of unfamiliar sources of intruders
D. An increase in the number of internally reported critical incidents

Answer: B

Explanation:
Signature-based intrusion detection systems (IDS) are systems that compare network traffic with predefined patterns of known attacks, called signatures. The effectiveness of signature-based IDS depends on how well they can detect new or unknown attacks that are not in their signature database. Therefore, an increase in the number of detected incidents not previously identified is the best indicator of the effectiveness of signature-based IDS, as it shows that they can recognize novel or modified attacks.

NEW QUESTION 189
- (Topic 2)
Which of the following will MOST likely compromise the control provided By a digital signature created using RSA encryption?

A. Reversing the hash function using the digest
B. Altering the plaintext message
C. Deciphering the receiver's public key
D. Obtaining the sender's private key

Answer: D

Explanation:
A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document, by using a hash function and an asymmetric encryption algorithm. A hash function is a mathematical function that transforms any input data into a fixed-length output value called a digest, which is unique for each input. An asymmetric encryption algorithm uses two keys: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret by the owner. To create a digital signature, the sender first applies a hash function to the plaintext message to generate a digest. Then, the sender encrypts the digest with their private key to produce the digital signature. To verify the digital signature, the receiver decrypts the digital signature with the sender's public key to obtain the digest. Then, the receiver applies the same hash function to the plaintext message to generate another digest. If the two digests match, it means that the message has not been altered and that it came from the sender. The security of a digital signature depends on the secrecy of the sender's private key. If an attacker obtains the sender's private key, they can create fake digital signatures for any message they want, thus compromising the control provided by the digital signature. Reversing the hash function using the digest is not possible, as hash functions are designed to be one-way functions that cannot be inverted. Altering the plaintext message will result in a different digest after applying the hash function, which will not match with the decrypted digest

from the digital signature, thus invalidating the digital signature. Deciphering the receiver’s public key is not relevant, as public keys are meant to be publicly available and do not affect the security of digital signatures.

NEW QUESTION 192
- (Topic 2)
An organization that has suffered a cyber-attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

A. An imaging process was used to obtain a copy of the data from each computer.
B. The legal department has not been engaged.
C. The chain of custody has not been documented.
D. Audit was only involved during extraction of the Information

Answer: C

Explanation:
The chain of custody has not been documented is a finding that should be of greatest concern for an IS auditor reviewing a forensic analysis process of an organization that has suffered a cyber attack. The chain of custody is a record of who handled, accessed, or modified the evidence during a forensic investigation. Documenting the chain of custody is essential to preserve the integrity, authenticity, and admissibility of the evidence in a court of law. The other options are less concerning findings that may not affect the validity or reliability of the forensic analysis process. References:
? CISA Review Manual (Digital Version), Chapter 7, Section 7.51
? CISA Review Questions, Answers & Explanations Database, Question ID 220

NEW QUESTION 193
- (Topic 2)
An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

A. Evaluate the appropriateness of the remedial action taken.
B. Conduct a risk analysis incorporating the change.
C. Report results of the follow-up to the audit committee.
D. Inform senior management of the change in approach.

Answer: A

Explanation:
The auditor’s next course of action should be to evaluate the appropriateness of the remedial action taken by the auditee. The auditor should assess whether the alternative approach taken by the auditee is effective, efficient, and aligned with the audit objectives and recommendations. The auditor should also consider the impact of the change on the audit scope, criteria, and risk assessment. Conducting a risk analysis incorporating the change, reporting results of the follow-up to the audit committee, and informing senior management of the change in approach are possible subsequent actions that the auditor may take after evaluating the appropriateness of the remedial action taken. References: CISA Review Manual (Digital Version): Chapter 1 - Information Systems Auditing Process

NEW QUESTION 198
- (Topic 2)
Which of the following should an IS auditor consider the MOST significant risk associated with a new health records system that replaces a legacy system?

A. Staff were not involved in the procurement process, creating user resistance to the new system.
B. Data is not converted correctly, resulting in inaccurate patient records.
C. The deployment project experienced significant overruns, exceeding budget projections.
D. The new system has capacity issues, leading to slow response times for users.

Answer: B

Explanation:
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as
significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition], page 281.

NEW QUESTION 203
- (Topic 1)
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 total transaction amount has no impact on financial reporting.
D. The retention period complies with data owner responsibilities.

Answer: D

Explanation:
The most important thing for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for the quality, security, and availability of the data under their control. They are also responsible for defining and enforcing data retention policies that comply with legal, regulatory, contractual, and business requirements. Data owners

should be consulted and involved in any decision that affects the retention period of their data, as they are ultimately liable for any consequences of data loss or breach.
The policy includes a strong risk-based approach, the retention period allows for review during the year-end audit, and the total transaction amount has no impact on financial reporting are not the most important things for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions. These are possible factors or benefits that may influence or justify the decision, but they do not override or replace the data owner responsibilities.

NEW QUESTION 207
- (Topic 1)
Which of the following is the MOST effective control to mitigate unintentional misuse of authorized access?

A. Annual sign-off of acceptable use policy
B. Regular monitoring of user access logs
C. Security awareness training
D. Formalized disciplinary action

Answer: C

Explanation:
The most effective control to mitigate unintentional misuse of authorized access is security awareness training. This is because security awareness training can educate users on the proper use of their access rights, the potential consequences of misuse, and the best practices to protect the confidentiality, integrity, and availability of information systems. Security awareness training can also help users recognize and avoid common threats such as phishing, malware, and social engineering.
Annual sign-off of acceptable use policy, regular monitoring of user access logs, and formalized disciplinary action are not the most effective controls to mitigate unintentional misuse of authorized access. These controls may help deter or detect intentional misuse, but they do not address the root cause of unintentional misuse, which is often a lack of knowledge or awareness of security policies and procedures.

NEW QUESTION 210
- (Topic 1)
Which of the following MOST effectively minimizes downtime during system conversions?

A. Phased approach
B. Direct cutover
C. Pilot study
D. Parallel run

Answer: D

Explanation:
The most effective way to minimize downtime during system conversions is to use a parallel run. A parallel run is a method of system conversion where both the old and new systems operate simultaneously for a period of time until the new system is verified to be functioning correctly. This reduces the risk of errors, data loss, or system failure during conversion and allows for a smooth transition from one system to another. References: CISA Review Manual, 27th Edition, page 467

NEW QUESTION 215
- (Topic 1)
Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

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

Answer: C

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

NEW QUESTION 217
......