Isaca

Exam Questions CISA

Isaca CISA

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
- (Topic 3)
What should an IS auditor do FIRST when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective?

A. Determine the resources required to make the control effective.
B. Validate the overall effectiveness of the internal control.
C. Verify the impact of the control no longer being effective.
D. Ascertain the existence of other compensating controls.

Answer: D

Explanation:
The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness. The other options are not the first steps, because they either require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

NEW QUESTION 2
- (Topic 3)
Which of the following is MOST important for an IS auditor to look for in a project feasibility study?

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

Answer: C

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

NEW QUESTION 3
- (Topic 3)
Which of the following IT service management activities is MOST likely to help with identifying the root cause of repeated instances of network latency?

A. Change management
B. Problem management
C. incident management
D. Configuration management

Answer: B

Explanation:
Problem management is an IT service management activity that is most likely to help with identifying the root cause of repeated instances of network latency. Problem management involves analyzing incidents that affect IT services and finding solutions to prevent them from recurring or minimize their impact. Change management is an IT service management activity that involves controlling and documenting any modifications to IT services or infrastructure. Incident management is an IT service management activity that involves restoring normal service operation as quickly as possible after an incident has occurred. Configuration management is an IT service management activity that involves identifying and maintaining records of IT assets and their relationships. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 334

NEW QUESTION 4
- (Topic 3)
Which of the following would BEST ensure that a backup copy is available for restoration of mission critical data after a disaster''

A. Use an electronic vault for incremental backups
B. Deploy a fully automated backup maintenance system.
C. Periodically test backups stored in a remote location
D. Use both tape and disk backup systems

Answer: C

Explanation:
The best way to ensure that a backup copy is available for restoration of mission critical data after a disaster is to periodically test backups stored in a remote location. Testing backups is essential to verify that the backup copies are valid, complete, and recoverable. Testing backups also helps to identify any issues or errors that may affect the backup process or the restoration of data. Storing backups in a remote location is important to protect the backup copies from physical damage, theft, or unauthorized access that may occur at the primary site. Using an electronic vault for incremental backups, deploying a fully automated backup maintenance system, or using both tape and disk backup systems are not sufficient to ensure that a backup copy is available for restoration of mission critical data

after a disaster, as they do not address the need for testing backups or storing them in a remote location. References: Backup and Recovery of Data: The Essential Guide | Veritas, The Truth About Data Backup for Mission-Critical Environments - DATAVERSITY.

NEW QUESTION 5
- (Topic 3)
Which of the following is a corrective control?

A. Separating equipment development testing and production
B. Verifying duplicate calculations in data processing
C. Reviewing user access rights for segregation
D. Executing emergency response plans

Answer: D

Explanation:
A corrective control is a control that aims to restore normal operations after a disruption or incident has occurred. Executing emergency response plans is an example of a corrective control, as it helps to mitigate the impact of an incident and resume business functions. Separating equipment development testing and production is a preventive control, as it helps to avoid errors or unauthorized changes in production systems. Verifying duplicate calculations in data processing is a detective control, as it helps to identify errors or anomalies in data processing. Reviewing user access rights for segregation is also a detective control, as it helps to detect any violations of segregation of duties principles. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 64

NEW QUESTION 6
- (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 7
- (Topic 3)
Which of the following is MOST critical for the effective implementation of IT governance?

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

Answer: C

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

NEW QUESTION 8
- (Topic 3)

An IS auditor reviewing the threat assessment tor a data center would be MOST concerned if:

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

Answer: C

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

NEW QUESTION 9
- (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 10
- (Topic 3)
An IS auditor follows up on a recent security incident and finds the incident response was not adequate. Which of the following findings should be considered MOST critical?

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

Answer: A

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

NEW QUESTION 10

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

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

Answer: C

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

NEW QUESTION 13
- (Topic 3)
Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

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

Answer: C

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

NEW QUESTION 15
- (Topic 3)
Which of the following BEST describes an audit risk?

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

Answer: B

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

NEW QUESTION 17
- (Topic 3)
An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which of two following is the MOST reliable follow- up procedure?

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

Answer: C

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

NEW QUESTION 22
- (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 26
- (Topic 3)
An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in- house. Which of the following findings should be the IS auditor's GREATEST concern?

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

Answer: D

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

NEW QUESTION 30
- (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 32
- (Topic 3)
An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider

MOST critical?

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

Answer: A

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

NEW QUESTION 33
- (Topic 3)
Which of the following is MOST important when implementing a data classification program?

A. Understanding the data classification levels
B. Formalizing data ownership
C. Developing a privacy policy
D. Planning for secure storage capacity

Answer: B

Explanation:
Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.
To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.
The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.
References:
? ISACA, CISA Review Manual, 27th Edition, 2020, page 247
? Data Classification: What It Is and How to Implement It

NEW QUESTION 36
- (Topic 2)
In a RAO model, which of the following roles must be assigned to only one individual?

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

Answer: D

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

NEW QUESTION 38
- (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 40
- (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 41
- (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 45
- (Topic 2)
The waterfall life cycle model of software development is BEST suited for which of the following situations?

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

Answer: A

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

NEW QUESTION 50
- (Topic 2)
Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

A. The job scheduler application has not been designed to display pop-up error messages.
B. Access to the job scheduler application has not been restricted to a maximum of two staff members
C. Operations shift turnover logs are not utilized to coordinate and control the processing environment
D. Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor

Answer: D

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

NEW QUESTION 53
- (Topic 2)
Which of the following is MOST important to consider when scheduling follow-up audits?

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

Answer: B

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

NEW QUESTION 57
- (Topic 2)
A now regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor's BEST recommendation to facilitate compliance with the regulation?

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

Answer: D

Explanation:
The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.
The other options are not as effective as including the requirement in the incident management response plan:
? Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.
? Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.
? Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

NEW QUESTION 58
- (Topic 2)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

Explanation:
The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical

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

NEW QUESTION 59
- (Topic 2)
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 63
- (Topic 2)
A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed Which of the following is the MOST important requirement to include In the vendor contract to ensure continuity?

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

Answer: C

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

NEW QUESTION 64
- (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 66
- (Topic 2)
Which of the following is a social engineering attack method?

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

Answer: A

Explanation:

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

NEW QUESTION 69
- (Topic 2)
An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

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

Answer: C

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

NEW QUESTION 72
- (Topic 2)
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

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

Answer: B

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

NEW QUESTION 77
- (Topic 2)
Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor's BEST recommendation for a compensating control?

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

Answer: A

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

staff members is a control that limits the number of people who can authorize payments, but it does not prevent them from initiating or processing payments themselves, which could violate SoD. Reconciling payment transactions with invoices is a control that verifies that the payments match the invoices, but it does not prevent unauthorized, duplicate or erroneous payments from being processed by the accounts payable system. Reviewing payment transaction history is a control that monitors and analyzes the payment transactions after they have been processed by the accounts payable system, but it does not prevent unauthorized, duplicate
or erroneous payments from occurring in the first place. References: CISA Review Manual
(Digital Version) , Chapter 5: Protection of Information Assets, Section 5.2: Logical Access.

NEW QUESTION 79
- (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 80
- (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 85
- (Topic 2)
During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related
to managing data risk. What should the auditor do FIRST?

A. Ask management why the regulatory changes have not been Included.
B. Discuss potential regulatory issues with the legal department
C. Report the missing regulatory updates to the chief information officer (CIO).
D. Exclude recent regulatory changes from the audit scope.

Answer: A

Explanation:
Asking management why the regulatory changes have not been included is the first thing that an IS auditor should do during the planning stage of a compliance audit. An IS auditor should inquire about the reasons for not updating the inventory of compliance requirements with recent regulatory changes related to managing data risk. This will help the IS auditor to understand whether there is a gap in awareness, communication, or implementation of compliance obligations

within the organization. The other options are not the first things that an IS auditor should do, but rather possible subsequent actions that may depend on management's response. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 214

NEW QUESTION 87
- (Topic 2)
Which of the following activities would allow an IS auditor to maintain independence while facilitating a control sell-assessment (CSA)?

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

Answer: D

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

NEW QUESTION 90
- (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 93
- (Topic 2)
During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

A. reflect current practices.
B. include new systems and corresponding process changes.
C. incorporate changes to relevant laws.
D. be subject to adequate quality assurance (QA).

Answer: A

Explanation:
The greatest concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated is that policies and procedures might not reflect current practices. Policies are documents that define the goals, objectives, and guidelines for an organization's information systems and resources. Procedures are documents that describe the steps, tasks, or activities for implementing or executing policies. Policies and procedures should be regularly reviewed and updated to ensure that they are relevant, accurate, consistent, and effective for the organization's information systems and resources. Policies and procedures that are not regularly reviewed and updated might not reflect current practices, as they might be outdated, obsolete, or incompatible with the current state or needs of the organization's information systems and resources. This can cause confusion, inconsistency, inefficiency, or noncompliance among users or stakeholders who rely on policies and procedures for guidance or direction. Policies and procedures might not include new systems and corresponding process changes is a possible concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated, but it is not the greatest one. Policies and procedures might not include new systems and corresponding process changes, as they might be unaware of or unresponsive to the introduction or modification of information systems or resources within the organization. This can cause gaps, overlaps, or conflicts among policies and procedures that affect different information systems or resources.

NEW QUESTION 98
- (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 101
- (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 102
- (Topic 2)
Which of the following must be in place before an IS auditor initiates audit follow-up activities?

A. Available resources for the activities included in the action plan
B. A management response in the final report with a committed implementation date
C. A heal map with the gaps and recommendations displayed in terms of risk
D. Supporting evidence for the gaps and recommendations mentioned in the audit report

Answer: B

Explanation:
This must be in place before an IS auditor initiates audit follow-up activities, because it indicates that management has acknowledged and accepted the audit findings and recommendations, and has agreed to take corrective actions within a specified timeframe. Audit follow-up activities are the processes and procedures that the IS auditor performs to verify that management has implemented the agreed-upon actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are not required to be in place before an IS auditor initiates audit follow- up activities:
? Available resources for the activities included in the action plan. This is a factor
that may affect the feasibility and success of the action plan, but it is not a prerequisite for the audit follow-up activities. The IS auditor should assess the availability and adequacy of the resources for the action plan during the audit planning and execution phases, and provide recommendations accordingly. However, the IS auditor does not need to wait for the resources to be available before initiating the audit follow-up activities.
? A heat map with the gaps and recommendations displayed in terms of risk. This is a tool that may help the IS auditor prioritize and communicate the gaps and recommendations, but it is not a requirement for the audit follow-up activities. A heat map is a graphical representation of data that uses colors to indicate the level of risk or impact of each gap or recommendation. The IS auditor may use a heat map to support the audit report or presentation, but it does not replace the need for a management response with a committed implementation date.
? Supporting evidence for the gaps and recommendations mentioned in the audit report. This is a component that should be included in the audit report, but it is not a condition for the audit follow-up activities. Supporting evidence is the information or data that supports or substantiates the audit findings and recommendations. The IS auditor should collect and document sufficient, reliable, relevant, and useful evidence during the audit execution phase, and present it in the audit report. However, the IS auditor does not need to have supporting evidence in place before initiating the audit follow-up activities.

NEW QUESTION 105
- (Topic 2)
Which of the following is the PRIMARY role of the IS auditor m an organization's information classification process?

A. Securing information assets in accordance with the classification assigned
B. Validating that assets are protected according to assigned classification
C. Ensuring classification levels align with regulatory guidelines
D. Defining classification levels for information assets within the organization

Answer: B

Explanation:
Validating that assets are protected according to assigned classification is the primary role of the IS auditor in an organization’s information classification process. An IS auditor should evaluate whether the information security controls are adequate and effective in safeguarding the information assets based on their classification levels. The other options are not the primary role of the IS auditor, but rather the responsibilities of the information owners, custodians, or security managers. References:

? CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 206

NEW QUESTION 107
- (Topic 1)
Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

A. Identifying relevant roles for an enterprise IT governance framework
B. Making decisions regarding risk response and monitoring of residual risk
C. Verifying that legal, regulatory, and contractual requirements are being met
D. Providing independent and objective feedback to facilitate improvement of IT processes

Answer: D

Explanation:
The most important benefit of involving IS audit when implementing governance of enterprise IT is providing independent and objective feedback to facilitate improvement of IT processes. Governance of enterprise IT is the process of ensuring that IT supports the organization’s strategy, goals, and objectives in an effective, efficient, ethical, and compliant manner. IS audit can provide value to governance of enterprise IT by assessing the alignment of IT with business needs, evaluating the performance and value delivery of IT, identifying risks and issues related to IT, recommending corrective actions and best practices, and monitoring the implementation and effectiveness of IT governance activities. IS audit can also provide assurance that IT governance processes are designed and operating in accordance with relevant standards, frameworks, laws, regulations, and contractual obligations. Identifying relevant roles for an enterprise IT governance framework is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help define and clarify the roles and responsibilities of various stakeholders involved in IT governance, such as board members, senior management, business units, IT function, external parties, etc. IS audit can also help ensure that these roles are aligned with the organization’s strategy, goals, and objectives, and that they have adequate authority, accountability, communication, and reporting mechanisms. However, this benefit is more related to the design phase of IT governance implementation than to the ongoing monitoring and improvement phase. Making decisions regarding risk response and monitoring of residual risk is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help identify and assess the risks associated with IT activities and processes, such as
strategic risks, operational risks, compliance risks, security risks, etc. IS audit can also help evaluate the effectiveness of risk management practices and controls implemented by management to mitigate or reduce these risks. However, this benefit is more related to the assurance function of IS audit than to its advisory function. Verifying that legal, regulatory, and contractual requirements are being met is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help verify that IT activities and processes comply with applicable laws, regulations, and contractual obligations, such as data protection laws, privacy laws, cybersecurity laws, industry standards, service level agreements, etc. IS audit can also help identify and report any instances of noncompliance or violations that could result in legal or reputational consequences for the organization. However, this benefit is more related to the assurance function of IS audit than to its advisory function. References: ISACA CISA Review Manual 27th Edition, page 283

NEW QUESTION 109
- (Topic 1)
Which of the following is the BEST control to prevent the transfer of files to external parties through instant messaging (IM) applications?

A. File level encryption
B. File Transfer Protocol (FTP)
C. Instant messaging policy
D. Application-level firewalls

Answer: D

Explanation:
Application level firewalls are the best control to prevent the transfer of files to external parties through instant messaging (IM) applications, because they can inspect and filter network traffic based on application-specific protocols and commands, such as IM file transfer commands. Application level firewalls can block or allow IM file transfers based on predefined rules or policies. File level encryption, file transfer protocol (FTP), and instant messaging policy are not effective controls to prevent IM file transfers, because they do not restrict or monitor IM network traffic. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.1

NEW QUESTION 111
- (Topic 1)
From an IS auditor's perspective, which of the following would be the GREATEST risk associated with an incomplete inventory of deployed software in an organization?

A. Inability to close unused ports on critical servers
B. Inability to identify unused licenses within the organization
C. Inability to deploy updated security patches
D. Inability to determine the cost of deployed software

Answer: C

Explanation:
The greatest risk associated with an incomplete inventory of deployed software in an organization is the inability to deploy updated security patches. Security patches are updates that fix vulnerabilities or bugs in software that could be exploited by attackers. Without an accurate inventory of software versions and configurations, it is difficult to identify and apply the relevant patches in a timely manner, which exposes the organization to increased security risks. Inability to close unused ports on critical servers, inability to identify unused licenses within the organization, and inability to determine the cost of deployed software are not as critical as security risks. References: ISACA CISA Review Manual 27th Edition, page 308

NEW QUESTION 112
- (Topic 1)
Which of the following would BEST facilitate the successful implementation of an IT-related framework?

A. Aligning the framework to industry best practices
B. Establishing committees to support and oversee framework activities

C. Involving appropriate business representation within the framework
D. Documenting IT-related policies and procedures

Answer: C

NEW QUESTION 113
- (Topic 1)
An organization has recently acquired and implemented intelligent-agent software for granting loans to customers. During the post-implementation review, which of the following is the MOST important procedure for the IS auditor to perform?

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

Answer: B

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

NEW QUESTION 117
- (Topic 1)
Coding standards provide which of the following?

A. Program documentation
B. Access control tables
C. Data flow diagrams
D. Field naming conventions

Answer: D

Explanation:
Coding standards provide field naming conventions, which are rules for naming variables, constants, functions, classes, and other elements in a program. Coding standards help to ensure consistency, readability, maintainability, and portability of code. Program documentation, access control tables, and data flow diagrams are not part of coding standards. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

NEW QUESTION 122
- (Topic 1)
Which of the following is the BEST detective control for a job scheduling process involving data transmission?

A. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management.
B. Jobs are scheduled to be completed daily and data is transmitted using a Secure File Transfer Protocol (SFTP).
C. Jobs are scheduled and a log of this activity is retained for subsequent review.
D. Job failure alerts are automatically generated and routed to support personnel.

Answer: D

Explanation:
The best detective control for a job scheduling process involving data transmission is job failure alerts that are automatically generated and routed to support personnel. Job failure alerts are notifications that indicate when a scheduled job or task fails to execute or complete successfully, such as due to errors, interruptions, or delays.
Job failure alerts can help detect and correct any issues or anomalies in the job scheduling process involving data transmission by informing and alerting the support personnel who can investigate and resolve the problem. The other options are not as effective as job failure alerts in detecting issues or anomalies in the job scheduling process involving data transmission, as they do not provide timely or specific information or feedback. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management is a reporting technique that can help measure and improve the performance and reliability of the job scheduling process, but it does not provide immediate or detailed information on individual job failures. Jobs are scheduled to be completed daily and data is transmitted using a Secure File Transfer Protocol (SFTP) is a preventive control that can help ensure the timeliness and security of the job scheduling process involving data transmission, but it does not detect any issues or anomalies that may occur during the process. Jobs are scheduled and a log of this activity is retained for subsequent review is a logging technique that can help record and track the status and results of the job scheduling process involving data transmission, but it does not provide real-time or proactive information on job failures. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 124
- (Topic 1)
Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

A. Frequent testing of backups
B. Annual walk-through testing
C. Periodic risk assessment
D. Full operational test

Answer: D

Explanation:
A disaster recovery plan (DRP) is a set of procedures and resources that enable an organization to restore its critical operations, data, and applications in the event of a disaster1. A DRP should be aligned with the organization's business continuity plan (BCP), which defines the strategies and objectives for maintaining

business functions during and after a disaster1.
To ensure that a DRP is effective, it should be tested regularly and thoroughly to identify and resolve any issues or gaps that might hinder its execution2345. Testing a DRP can help evaluate its feasibility, validity, reliability, and compatibility with the organization's environment and needs4. Testing can also help prepare the staff, stakeholders, and vendors involved in the DRP for their roles and responsibilities during a disaster3. There are different methods and levels of testing a DRP, depending on the scope, complexity, and objectives of the test4. Some of the common testing methods are:
? Walkthrough testing: This is a step-by-step review of the DRP by the disaster
recovery team and relevant stakeholders. It aims to verify the completeness and accuracy of the plan, as well as to clarify any doubts or questions among the participants45.
? Simulation testing: This is a mock exercise of the DRP in a simulated disaster scenario. It aims to assess the readiness and effectiveness of the plan, as well as to identify any challenges or weaknesses that might arise during a real disaster45.
? Checklist testing: This is a verification of the availability and functionality of the resources and equipment required for the DRP. It aims to ensure that the backup systems, data, and documentation are accessible and up-to-date45.
? Full interruption testing: This is the most realistic and rigorous method of testing a DRP. It involves shutting down the primary site and activating the backup site for a certain period of time. It aims to measure the actual impact and performance of the DRP under real conditions45.
? Parallel testing: This is a less disruptive method of testing a DRP. It involves running the backup site in parallel with the primary site without affecting the normal operations. It aims to compare and validate the results and outputs of both sites45.
Among these methods, full interruption testing would best demonstrate that an effective DRP is in place, as it provides the most accurate and comprehensive evaluation of the plan's capabilities and limitations4. Full interruption testing can reveal any hidden or unforeseen issues or risks that might affect the recovery process, such as data loss, system failure, compatibility problems, or human errors4. Full interruption testing can also verify that the backup site can support the critical operations and services of the organization without compromising its quality or security4.
However, full interruption testing also has some drawbacks, such as being costly, time- consuming, risky, and disruptive to the normal operations4. Therefore, it should be planned carefully and conducted periodically with proper coordination and communication among all parties involved4.
The other options are not as effective as full interruption testing in demonstrating that an effective DRP is in place. Frequent testing of backups is only one aspect of checklist testing, which does not cover other components or scenarios of the DRP4. Annual walk- through testing is only a theoretical review of the DRP, which does not test its practical implementation or outcomes4. Periodic risk assessment is only a preparatory step for developing or updating the DRP, which does not test its functionality or performance4. References: 2: Best Practices For Disaster Recovery Testing | Snyk 3: Disaster Recovery Plan (DR) Testing — Methods and Must-haves - US Signal 4: Disaster Recovery Testing: What You Need to Know - Enterprise Storage Forum 5: Disaster Recovery Testing Best Practices - MSP360 1: How to Test a Disaster Recovery Plan - Abacus

NEW QUESTION 127
- (Topic 1)
When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:

A. a risk management process.
B. an information security framework.
C. past information security incidents.
D. industry best practices.

Answer: A

Explanation:
Information security policies are high-level statements that define the organization's approach to protecting its information assets from threats and risks. They should be based primarily on a risk management process, which is a systematic method of identifying, analyzing, evaluating, treating, and monitoring information security risks. A risk management process can help ensure that the policies are aligned with the organization's risk appetite, business objectives, legal and regulatory requirements, and stakeholder expectations. An information security framework is a set of standards, guidelines, and best practices that provide a structure for implementing information security policies. It can support the risk management process, but it is not the primary basis for defining the policies. Past information security incidents and industry best practices can also provide valuable inputs for defining the policies, but they are not sufficient to address the organization's specific context and needs. References: Insights and Expertise, CISA Review Manual (Digital Version)

NEW QUESTION 129
- (Topic 1)
During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

A. allocation of resources during an emergency.
B. frequency of system testing.
C. differences in IS policies and procedures.
D. maintenance of hardware and software compatibility.

Answer: A

Explanation:
During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be most concerned with the allocation of resources during an emergency. A reciprocal disaster recovery agreement is an arrangement by which one organization agrees to use another's resources in the event of a business continuity event or incident. The IS auditor would need to ensure that both parties have clearly defined their roles and responsibilities, their resource requirements, their priority levels, their communication channels, and their escalation procedures in case of a disaster. The IS auditor would also need to verify that both parties have tested their agreement and have updated it regularly to reflect any changes in their business environments. The frequency of system testing is not as critical as the allocation of resources during an emergency, because system testing can be performed periodically or on demand, while resource allocation is a dynamic and complex process that requires careful planning and coordination. The differences in IS policies and procedures are not as critical as the allocation of resources during an emergency, because both parties can agree on common standards and protocols for their disaster recovery operations, or they can adapt their policies and procedures to suit each other's needs. The maintenance of hardware and software compatibility is not as critical as the allocation of resources during an emergency, because both parties can use compatible or interoperable systems, or they can use virtualization or cloud computing technologies to overcome any compatibility issues. References: ISACA CISA Review Manual 27th Edition, page 281

NEW QUESTION 133
- (Topic 1)
Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

A. Audit cycle defined in the audit plan
B. Complexity of management's action plans
C. Recommendation from executive management

D. Residual risk from the findings of previous audits

Answer: D

Explanation:
Residual risk from the findings of previous audits should be the primary basis for prioritizing follow-up audits, because it reflects the level of exposure and potential impact that remains after management has implemented corrective actions or accepted the risk. Follow-up audits should focus on verifying whether the residual risk is within acceptable levels and whether the corrective actions are effective and sustainable. Audit cycle defined in the audit plan, complexity of management's action plans, and recommendation from executive management are not valid criteria for prioritizing follow-up audits, because they do not consider the residual risk from previous audits. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.4.3

NEW QUESTION 134
- (Topic 1)
Which of the following strategies BEST optimizes data storage without compromising data retention practices?

A. Limiting the size of file attachments being sent via email
B. Automatically deleting emails older than one year
C. Moving emails to a virtual email vault after 30 days
D. Allowing employees to store large emails on flash drives

Answer: A

Explanation:
The best strategy to optimize data storage without compromising data retention practices is to limit the size of file attachments being sent via email. This strategy can reduce the amount of storage space required for email messages, as well as the network bandwidth consumed by email traffic. File attachments can be large and often contain redundant or unnecessary information that can be compressed, converted, or removed before sending. By limiting the size of file attachments, the sender can encourage the use of more efficient formats, such as PDF or ZIP, or alternative methods of sharing files, such as cloud storage or web links. This can also improve the security and privacy of email communications, as large attachments may pose a higher risk of being intercepted, corrupted, or infected by malware.
References:
? Data Storage Optimization: What is it and Why Does it Matter?
? Data storage optimization 101: Everything you need to know

NEW QUESTION 136
- (Topic 1)
A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

A. Periodically reviewing log files
B. Configuring the router as a firewall
C. Using smart cards with one-time passwords
D. Installing biometrics-based authentication

Answer: A

Explanation:
The most effective way to detect an intrusion attempt is to periodically review log files, which record the activities and events on a system or network. Log files can provide evidence of unauthorized access attempts, malicious activities, or system errors. Configuring the router as a firewall, using smart cards with one-time passwords, and installing biometrics-based authentication are preventive controls that can reduce the likelihood of an intrusion, but they do not detect it.
References: ISACA CISA Review Manual 27th Edition, page 301

NEW QUESTION 137
- (Topic 1)
Which of the following is MOST important to include in forensic data collection and preservation procedures?

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

Answer: B

Explanation:
The most important thing to include in forensic data collection and preservation procedures is preserving data integrity. Data integrity is the property that ensures that data is accurate, complete, and consistent throughout its lifecycle. Preserving data integrity is essential for forensic data collection and preservation procedures because it ensures that the data can be used as valid and reliable evidence in legal proceedings or investigations. Preserving data integrity can be achieved by using methods such as hashing, checksums, digital signatures, write blockers, tamper-evident seals, or timestamps. The other options are not as important as preserving data integrity in forensic data collection and preservation procedures, as they do not affect the validity or reliability of the data. Assuring the physical security of devices is a security measure that protects devices from unauthorized access, theft, damage, or destruction, but it does not ensure that the data on the devices is accurate, complete, and consistent. Maintaining chain of custody is a documentation technique that records and tracks the handling and transfer of devices or data among different parties involved in forensic activities, but it does not ensure that the data on the devices is accurate, complete, and consistent. Determining tools to be used is a planning activity that selects and prepares the appropriate tools for forensic data collection and preservation procedures, but it does not ensure that the data collected and preserved by the tools is accurate, complete, and consistent. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION 140
- (Topic 1)
Cross-site scripting (XSS) attacks are BEST prevented through:

A. application firewall policy settings.
B. a three-tier web architecture.
C. secure coding practices.
D. use of common industry frameworks.

Answer: C

Explanation:
Secure coding practices are the best way to prevent cross-site scripting (XSS) attacks, because they can ensure that the web application validates and sanitizes user input and output data to prevent malicious scripts from being executed on the web browser. XSS attacks are a type of web application vulnerability that exploit the lack of input validation or output encoding in web pages that accept user input or display dynamic content. Application firewall policy settings, a three-tier web architecture, and use of common industry frameworks are not effective controls to prevent XSS attacks, because they do not address the root cause of the vulnerability in the web application code. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

NEW QUESTION 144
- (Topic 1)
Which of the following fire suppression systems needs to be combined with an automatic switch to shut down the electricity supply in the event of activation?

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

Answer: A

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

NEW QUESTION 146
- (Topic 1)
An incorrect version of the source code was amended by a development team. This MOST likely indicates a weakness in:

A. incident management.
B. quality assurance (QA).
C. change management.
D. project management.

Answer: C

Explanation:
A weakness in change management is the most likely cause of an incorrect version of source code being amended by a development team. Change management is the process of controlling and documenting changes to IT systems and software. It ensures that changes are authorized, tested, and implemented in a controlled manner. If change management is weak, there is a risk of using outdated or incorrect versions of source code, which can lead to errors, defects, or security vulnerabilities in the software.

NEW QUESTION 147
- (Topic 1)
A proper audit trail of changes to server start-up procedures would include evidence of:

A. subsystem structure.
B. program execution.
C. security control options.
D. operator overrides.

Answer: D

Explanation:
A proper audit trail of changes to server start-up procedures would include evidence of operator overrides, which are actions taken by the system operator to bypass or modify the normal execution of the server start-up process. Operator overrides may indicate unauthorized or improper changes that could affect the security, availability, or performance of the server. Therefore, an audit trail should capture and document any operator overrides that occur during the server start-up process.
Evidence of subsystem structure, program execution, and security control options are not directly related to changes to server start-up procedures. Subsystem structure refers to the components and relationships of a subsystem within a larger system. Program execution refers to the process of running a software program on a computer. Security control options refer to the settings and parameters that define the security level and access rights for a system or application. These are all important aspects of auditing a server, but they do not provide evidence of changes to server start-up procedures.

NEW QUESTION 148
- (Topic 1)
An IS auditor discovers that validation controls m a web application have been moved from the server side into the browser to boost performance This would MOST likely increase the
risk of a successful attack by.

A. phishing.
B. denial of service (DoS)
C. structured query language (SQL) injection
D. buffer overflow

Answer: C

Explanation:
Moving validation controls from the server side into the browser would most likely increase the risk of a successful attack by structured query language (SQL) injection. SQL injection is a technique that exploits a security vulnerability in an application's database layer by inserting malicious SQL statements into user input fields. Validation controls are used to check and filter user input before sending it to the database. If these controls are moved to the browser, they can be easily bypassed or modified by an attacker, who can then execute arbitrary SQL commands on the database. References: CISA Review Manual, 27th Edition, page 361

NEW QUESTION 150
- (Topic 1)
Which of the following is MOST important for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros?

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

Answer: C

Explanation:
The most important thing for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros is the formulas within macros. Macros are sequences of commands or instructions that can automate tasks or calculations in a spreadsheet. Formulas are expressions that perform calculations on values or data in a spreadsheet. The accuracy of a spreadsheet depends largely on whether the formulas within macros are correct, consistent, and complete. The IS auditor should review the formulas within macros to verify that they produce the expected results and do not contain any errors or inconsistencies. The other options are not as important as formulas within macros, as they do not directly affect the accuracy of a spreadsheet. Encryption of the spreadsheet is a security control that can protect the confidentiality and integrity of the spreadsheet, but it does not ensure its accuracy. Version history is a document control feature that can track and manage changes to the spreadsheet, but it does not verify its accuracy. Reconciliation of key calculations is a validation technique that can compare and confirm the results of calculations with other sources, but it does not evaluate the accuracy of formulas within macros. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION 152
- (Topic 1)
An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

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

Answer: D

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

NEW QUESTION 157
- (Topic 3)
Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

A. Perimeter firewall
B. Data loss prevention (DLP) system
C. Web application firewall
D. Network segmentation

Answer: D

Explanation:
Network segmentation is the best security measure to reduce the risk of propagation when a cyberattack occurs, because it divides the network into smaller subnetworks that are isolated from each other and have different access controls and security policies. This limits the spread of malicious traffic and prevents attackers from accessing sensitive data or systems in other segments. A perimeter firewall, a data loss prevention (DLP) system, and a web application firewall are also useful security measures, but they do not prevent propagation within the network as effectively as network segmentation does. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

NEW QUESTION 158
- (Topic 3)
Which of the following should be the FIRST step in the incident response process for a suspected breach?

A. Inform potentially affected customers of the security breach
B. Notify business management of the security breach.
C. Research the validity of the alerted breach
D. Engage a third party to independently evaluate the alerted breach.

Answer: C

Explanation:

The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the incident response process, but they are not the first step. References:
? CISA Review Manual, 27th Edition, page 4251
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 159
- (Topic 3)
Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?

A. Program coding standards have been followed
B. Acceptance test criteria have been developed
C. Data conversion procedures have been established.
D. The design has been approved by senior management.

Answer: B

Explanation:
The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase. Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 323

NEW QUESTION 160
- (Topic 3)
Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

A. Inability to utilize the site when required
B. Inability to test the recovery plans onsite
C. Equipment compatibility issues at the site
D. Mismatched organizational security policies

Answer: A

Explanation:
The greatest risk of using a reciprocal site for disaster recovery is the inability to utilize the site when required. A reciprocal site is an agreement between two organizations to provide backup facilities for each other in case of a disaster. However, this arrangement may not be reliable or enforceable, especially if both organizations are affected by the same disaster or have conflicting priorities. Therefore, the IS auditor should recommend that management consider alternative options for disaster recovery, such as dedicated sites or cloud services12. References:
? CISA Review Manual, 27th Edition, page 3381
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 161
- (Topic 3)
Which of the following backup schemes is the BEST option when storage media is limited?

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

Answer: C

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

NEW QUESTION 166
- (Topic 3)
An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

A. Loss of application support
B. Lack of system integrity
C. Outdated system documentation
D. Developer access 1o production

Answer: B

Explanation:
The most significant risk from not testing patches before putting them into production is the lack of system integrity. Patches are software updates that fix bugs,

vulnerabilities or performance issues in an application system. However, patches may also introduce new errors, conflicts or compatibility issues that could affect the functionality, reliability or security of the system4. By not testing patches before putting them into production, the organization exposes itself to the risk of system failures, data corruption or unauthorized access. Loss of application support, outdated system documentation and developer access to production are also risks from not testing patches, but they are not as significant as the lack of system integrity. References:
? CISA Review Manual, 27th Edition, page 2951
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION 171
- (Topic 3)
Which of the following would MOST effectively help to reduce the number of repealed incidents in an organization?

A. Testing incident response plans with a wide range of scenarios
B. Prioritizing incidents after impact assessment.
C. Linking incidents to problem management activities
D. Training incident management teams on current incident trends

Answer: C

Explanation:
Linking incidents to problem management activities would most effectively help to reduce the number of repeated incidents in an organization, because problem management aims to identify and eliminate the root causes of incidents and prevent their recurrence. Testing incident response plans, prioritizing incidents, and training incident management teams are all good practices, but they do not directly address the issue of repeated incidents. References: ISACA ITAF 3rd Edition Section 3600

NEW QUESTION 176
- (Topic 3)
A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

A. Using smart cards with one-time passwords
B. Periodically reviewing log files
C. Configuring the router as a firewall
D. Installing biometrics-based authentication

Answer: B

Explanation:
Periodically reviewing log files is the most effective way to detect intrusion attempts from outside the organization, as they can provide evidence of unauthorized access attempts, source IP addresses, timestamps and other relevant information. Using smart cards with one-time passwords or installing biometrics-based authentication can prevent unauthorized access, but not detect it. Configuring the router as a firewall can block unwanted traffic, but not log it. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 361

NEW QUESTION 177
- (Topic 3)
Which of the following would provide an IS auditor with the GREATEST assurance that data disposal controls support business strategic objectives?

A. Media recycling policy
B. Media sanitization policy
C. Media labeling policy
D. Media shredding policy

Answer: B

Explanation:
Data disposal controls are the measures that ensure that data are securely and permanently erased or destroyed when they are no longer needed or authorized to be retained. Data disposal controls support business strategic objectives by reducing the risk of data breaches, complying with data privacy regulations, optimizing the use of storage resources, and enhancing the reputation and trust of the organization1.
A media sanitization policy is a document that defines the roles, responsibilities, procedures, and standards for sanitizing different types of media that contain sensitive or confidential data. Media sanitization is the process of removing or modifying data on a media device to make it unreadable or unrecoverable by any means. Media sanitization can be achieved by various methods, such as overwriting, degaussing, encryption, or physical destruction2.
A media sanitization policy would provide an IS auditor with the greatest assurance that data disposal controls support business strategic objectives because it demonstrates that the organization has a clear and consistent approach to protect its data from unauthorized access or disclosure throughout the data life cycle. A media sanitization policy also helps the organization to comply with various data privacy regulations, such as the EU General Data Protection Regulation (GDPR), the US Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS), that require proper disposal of personal or sensitive data3.
The other options are not as effective as a media sanitization policy in providing assurance that data disposal controls support business strategic objectives. A media recycling policy is a document that defines the criteria and procedures for reusing media devices that have been sanitized or erased. A media recycling policy can help the organization to save costs and reduce environmental impact, but it does not address how the data are disposed of in the first place4. A media labeling policy is a document that defines the rules and standards for labeling media devices that contain sensitive or confidential data. A media labeling policy can help the organization to identify and classify its data assets, but it does not specify how the data are sanitized or destroyed when they are no longer needed. A media shredding policy is a document that defines the methods and procedures for physically destroying media devices that contain sensitive or confidential data. A media shredding policy can be a part of a media sanitization policy, but it is not sufficient to cover all types of media devices or data disposal scenarios.
References:
? ISACA, CISA Review Manual, 27th Edition, 2019
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
? Secure Data Disposal and Destruction: 6 Methods to Follow1
? Why (and How to) Dispose of Digital Data2
? What is Data Disposition? The Complete Guide3
? Data Disposition: What is it and why should it be part of your data retention policy?

NEW QUESTION 180
- (Topic 3)
What should an IS auditor do FIRST upon discovering that a service provider did not notify its customers of a security breach?

A. Notify law enforcement of the finding.
B. Require the third party to notify customers.
C. The audit report with a significant finding.
D. Notify audit management of the finding.

Answer: D

Explanation:
The IS auditor should notify audit management of the finding first, as this is a significant issue that may affect the audit scope and objectives. The IS auditor should not notify law enforcement or require the third party to notify customers without consulting audit management first. The audit report with a significant finding should be issued after the audit is completed and the findings are validated. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 247

NEW QUESTION 185
- (Topic 1)
Which of the following BEST ensures the quality and integrity of test procedures used in audit analytics?

A. Developing and communicating test procedure best practices to audit teams
B. Developing and implementing an audit data repository
C. Decentralizing procedures and Implementing periodic peer review
D. Centralizing procedures and implementing change control

Answer: D

Explanation:
The best way to ensure the quality and integrity of test procedures used in audit analytics is to centralize procedures and implement change control. Centralizing procedures means storing them in a common repository that can be accessed and updated by authorized users. Change control means implementing a process for tracking, reviewing, approving, and documenting any changes made to the procedures. This ensures that the procedures are consistent, accurate, reliable, and secure. References:
CISA Review Manual, 27th Edition, page 401

NEW QUESTION 188
- (Topic 1)
The PRIMARY benefit lo using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

A. is more effective at suppressing flames.
B. allows more time to abort release of the suppressant.
C. has a decreased risk of leakage.
D. disperses dry chemical suppressants exclusively.

Answer: C

Explanation:
The primary benefit of using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system has a decreased risk of leakage, as the pipes are filled with pressurized air or nitrogen instead of water until the system is activated. A wet- pipe system has a higher risk of leakage, corrosion, and freezing. A dry-pipe system is not more effective at suppressing flames, as it uses the same water-based suppressant as a wet-pipe system. A dry-pipe system does not allow more time to abort release of the suppressant, as it has a delay of only a few seconds before the water is released. A dry- pipe system does not disperse dry chemical suppressants exclusively, as it uses water as the primary suppressant. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.3

NEW QUESTION 193
......

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

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

Contact us

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

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