

# Isaca

## Exam Questions CISA

Isaca CISA



### NEW QUESTION 1

- (Topic 3)

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

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

**Answer:** D

#### Explanation:

The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use. A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data<sup>1</sup>. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personal accounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.

The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.

References:

? ISACA CISA Review Manual 27th Edition (2019), page 247

? What is a Security Policy? Definition, Elements, and Examples - Varonis<sup>1</sup>

### NEW QUESTION 2

- (Topic 3)

Which of the following should be of GREATEST concern to an IS auditor reviewing a network printer disposal process?

- A. Disposal policies and procedures are not consistently implemented
- B. Evidence is not available to verify printer hard drives have been sanitized prior to disposal.
- C. Business units are allowed to dispose printers directly to
- D. Inoperable printers are stored in an unsecured area.

**Answer:** B

#### Explanation:

The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 387

### NEW QUESTION 3

- (Topic 3)

Which of the following is MOST important for an IS auditor to look for in a project feasibility study?

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

**Answer:** C

#### Explanation:

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

CISA Review Manual (Digital Version)<sup>1</sup>, Chapter 4, Section 4.2.1

### NEW QUESTION 4

- (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 5**

- (Topic 3)

Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

- A. Ensure that paper documents are disposed securely.
- B. Implement an intrusion detection system (IDS).
- C. Verify that application logs capture any changes made.
- D. Validate that all data files contain digital watermarks

**Answer: D**

**Explanation:**

Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data leakage by deterring potential leakers from sharing sensitive data or by providing evidence of data leakage if it occurs.

The other options are not as effective as digital watermarks in preventing data leakage. Ensuring that paper documents are disposed securely can reduce the risk of physical data leakage, but it does not address the digital data leakage that is more prevalent in today's environment. Implementing an intrusion detection system (IDS) can help detect and respond to cyberattacks that may cause data leakage, but it does not prevent data leakage from insiders or authorized users who have legitimate access to the data. Verifying that application logs capture any changes made can help audit and investigate data leakage incidents, but it does not prevent them from happening in the first place.

References:

- ? What is Data Leakage?
- ? What is Digital Watermarking?

**NEW QUESTION 6**

- (Topic 3)

An IS auditor finds that capacity management for a key system is being performed by IT with no input from the business. The auditor's PRIMARY concern would be:

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 7**

- (Topic 3)

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

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

**Answer: D**

**Explanation:**

The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources, procedures, communication plans, and backup arrangements<sup>3</sup>. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements. Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident<sup>4</sup>. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:

? A. The BCP's contact information needs to be updated is not a great concern for an IS auditor reviewing an organization's BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.

? B. The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization's BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or effectiveness of the BCP.

? C. The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization's BCP, as it is a high-level issue

that can be resolved. Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization. Approval by senior management helps to ensure that the BCP is aligned with the organization's strategy, objectives, and priorities, and that it has sufficient resources and authority to be implemented. Approval by senior management also helps to increase the awareness and commitment of the organization's stakeholders to the BCP. While having no approval by senior management may affect the credibility and acceptance of the BCP, it does not affect the overall validity or effectiveness of the BCP. References: Working Toward a Managed, Mature Business Continuity Plan - ISACA, ISACA Introduces New Audit Programs for Business Continuity/Disaster ..., Disaster Recovery and Business Continuity Preparedness for Cloud-based ...

#### NEW QUESTION 8

- (Topic 3)

Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

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

**Answer: A**

#### Explanation:

An appropriate role of internal audit in helping to establish an organization's privacy program is analyzing risks posed by new regulations. A privacy program is a set of policies, procedures, and controls that aim to protect the personal data of individuals from unauthorized or unlawful collection, use, disclosure, or disposal. A privacy program should comply with the applicable laws and regulations that govern the privacy rights and obligations of individuals and organizations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). New regulations may introduce new requirements or changes that affect the organization's privacy program and expose it to potential compliance risks or penalties. Therefore, internal audit can help to establish an organization's privacy program by analyzing the risks posed by new regulations and providing assurance, advice, or recommendations on how to address them<sup>1</sup>. The other options are less appropriate or incorrect because:

? B. Developing procedures to monitor the use of personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the effectiveness and efficiency of the organization's privacy program, but not create or execute it<sup>2</sup>.

? C. Defining roles within the organization related to privacy is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a governance or strategic role. Internal audit should not be involved in setting or approving the organization's privacy strategy, objectives, or policies, as it would compromise its independence and objectivity. Internal audit should provide assurance on the alignment and compliance of the organization's privacy program with its strategy, objectives, and policies, but not define or approve them<sup>2</sup>.

? D. Designing controls to protect personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the adequacy and effectiveness of the organization's privacy program, but not design or implement it<sup>2</sup>. References: ISACA Introduces New Audit Programs for Business Continuity/Disaster ..., Best Practices for Privacy Audits - ISACA, ISACA Produces New Audit and Assurance Programs for Data Privacy and ...

#### NEW QUESTION 9

- (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 10

- (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 10

- (Topic 3)

An IS auditor discovers that an IT organization serving several business units assigns equal priority to all initiatives, creating a risk of delays in securing project funding. Which of the following would be MOST helpful in matching demand for projects and services with available resources in a way that supports business objectives?

- A. Project management
- B. Risk assessment results
- C. IT governance framework
- D. Portfolio management

**Answer: D**

**Explanation:**

The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management. Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and services with the strategic goals and value proposition of the organization<sup>3</sup>. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services. References:

? CISA Review Manual, 27th Edition, page 721

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

**NEW QUESTION 12**

- (Topic 3)

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

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

**Answer: A**

**Explanation:**

The approach adopted by management in this scenario is risk avoidance. Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a threat to the organization<sup>3</sup>. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case. References:

? CISA Review Manual, 27th Edition, page 641

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

**NEW QUESTION 13**

- (Topic 3)

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

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

**Answer: B**

**Explanation:**

Developing a risk-based plan considering each entity's business processes would best help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk-based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders<sup>1</sup>. By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope, and procedures accordingly. This can help to address the unique needs and expectations of each entity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance<sup>2</sup>.

The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.

References:

? ISACA, CISA Review Manual, 27th Edition, 2019

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

? Risk-Based Audit Planning: A Guide for Internal Audit<sup>1</sup>

? Risk-Based Audit Approach: Definition & Example

**NEW QUESTION 14**

- (Topic 3)

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

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

D. the information owner is required to approve access to the asset

**Answer: B**

**Explanation:**

When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements. The security criteria should define the level of confidentiality, integrity, and availability for each data classification, as well as the corresponding controls such as access control, rights management, and cryptographic protection<sup>1</sup>. The other options are less important or incorrect because:  
 ? A. Each information asset is not necessarily assigned to a different classification. Data classification schemes usually have a limited number of categories, such as "Sensitive," "Confidential," and "Public," and multiple information assets can belong to the same category<sup>2</sup>.  
 ? C. Senior IT managers are not necessarily identified as information owners. Information owners are typically the business units or functions that create, use, or maintain the information assets, and they may or may not be senior IT managers<sup>3</sup>.  
 ? D. The information owner is not required to approve access to the asset. The information owner is responsible for defining the access requirements and rules for the asset, but the actual approval of access requests may be delegated to other roles, such as data custodians or administrators<sup>3</sup>.  
 References: Simplify and Contextualize Your Data Classification Efforts - ISACA, 3.7: Establish and Maintain a Data Classification Scheme, Data Classification and Practices - NIST, CISA Exam Content Outline | CISA Certification | ISACA

**NEW QUESTION 19**

- (Topic 3)

An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 23**

- (Topic 3)

What is the BEST method to determine if IT resource spending is aligned with planned project spending?

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

**Answer: A**

**Explanation:**

The best method to determine if IT resource spending is aligned with planned project spending is earned value analysis (EVA). EVA is a technique that compares the actual cost, schedule, and scope of a project with the planned or budgeted values. EVA can help to measure the project progress and performance, and identify any variances or deviations from the baseline plan<sup>1</sup>.  
 EVA uses three basic values to calculate the project status: planned value (PV), earned value (EV), and actual cost (AC). PV is the amount of work that was expected to be completed by a certain date, according to the project plan. EV is the amount of work that was actually completed by that date, measured in terms of the budgeted cost. AC is the amount of money that was actually spent to complete the work by that date<sup>1</sup>.  
 By comparing these values, EVA can determine if the project is on track, ahead, or behind schedule and budget. EVA can also calculate various indicators, such as cost variance (CV), schedule variance (SV), cost performance index (CPI), and schedule performance index (SPI), to quantify the magnitude and direction of the variances. EVA can also forecast the future performance and completion of the project, based on the current trends and assumptions<sup>1</sup>.  
 The other options are not as effective as EVA in determining if IT resource spending is aligned with planned project spending. Option B, return on investment (ROI) analysis, is a technique that evaluates the profitability or efficiency of an investment, by comparing the benefits or revenues with the costs. ROI analysis can help to justify or prioritize a project, but it does not measure the actual progress or performance of the project against the plan<sup>2</sup>. Option C, Gantt chart, is a tool that displays the tasks, durations, dependencies, and milestones of a project in a graphical format. Gantt chart can help to plan and monitor a project schedule, but it does not show the actual cost or scope of the project<sup>3</sup>. Option D, critical path analysis, is a technique that identifies the longest sequence of tasks or activities that must be completed on time for the project to finish on schedule. Critical path analysis can help to optimize and control a project schedule, but it does not account for the actual cost or scope of the project<sup>4</sup>.  
 References:  
 ? Earned Value Analysis & Management (EVA/EVM) – Definition & Formulae<sup>1</sup>  
 ? Return on Investment (ROI) Formula<sup>2</sup>  
 ? What Is a Gantt Chart?<sup>3</sup>  
 ? Critical Path Method for Project Management

**NEW QUESTION 27**

- (Topic 3)

An IS auditor finds that the process for removing access for terminated employees is not documented. What is the MOST significant risk from this observation?

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

Answer: D

**Explanation:**

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 32**

- (Topic 3)

An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

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

Answer: C

**Explanation:**

The major concern with the situation where security incidents are resolved and closed, but root causes are not investigated, is that vulnerabilities have not been properly addressed. Vulnerabilities are weaknesses or gaps in the security posture of an organization that can be exploited by threat actors to compromise its systems, data, or operations. If root causes are not investigated, vulnerabilities may remain undetected or unresolved, allowing attackers to exploit them again or use them as entry points for further attacks. This can result in repeated or escalated security incidents that can cause more damage or disruption to the organization.

The other options are not as major as the concern about vulnerabilities, but rather secondary or related issues that may arise from the lack of root cause analysis. Abuses by employees have not been reported is a concern that may indicate a lack of awareness, accountability, or monitoring of insider threats. Lessons learned have not been properly documented is a concern that may indicate a lack of improvement, learning, or feedback from security incidents. Security incident policies are out of date is a concern that may indicate a lack of alignment, review, or update of security incident processes.

References:

? ISACA CISA Review Manual 27th Edition (2019), page 254

? Why Root Cause Analysis is Crucial to Incident Response (IR) - Avertium3

? Root Cause Analysis Steps and How it Helps Incident Response ...

**NEW QUESTION 35**

- (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 identify as the associated risk?

- A. The use of the cloud negatively impacting IT availability
- 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 location<sup>6</sup>. 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 devices<sup>7</sup>. 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 compromise<sup>8</sup>. 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 36**

- (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 38**

- (Topic 3)

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

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

**Answer: B**

**Explanation:**

Partitioning the work environment from personal space on devices. This would best maintain information security without compromising employee privacy by creating a separate and secure area on the personal mobile devices for work-related data and applications. This way, the organization can protect its information from unauthorized access, loss, or leakage, while respecting the employees' personal data and preferences on their own devices.

The other options are not as effective as option B in balancing information security and employee privacy. Option A, installing security software on the devices, is a good practice but may not be sufficient to prevent data breaches or comply with regulatory requirements. Option C, preventing users from adding applications, is too restrictive and may interfere with the employees' personal use of their devices. Option D, restricting the use of devices for personal purposes during working hours, is impractical and difficult to enforce. References:

- ? ISACA, CISA Review Manual, 27th Edition, 2019
- ? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
- ? Personal Cellphone Privacy at Work<sup>1</sup>
- ? Protecting your personal information and privacy on a company phone<sup>2</sup>
- ? Mobile Devices and Protected Health Information (PHI)<sup>3</sup>
- ? Using your personal phone for work? Here's how to separate your apps and data<sup>4</sup>
- ? 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work<sup>5</sup>

**NEW QUESTION 40**

- (Topic 3)

An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

- A. Improve the change management process
- B. Establish security metrics.
- C. Perform a penetration test
- D. Perform a configuration review

**Answer: D**

**Explanation:**

The best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities is to perform a configuration review. A configuration review is an audit procedure that involves examining and verifying the security settings and parameters of application servers against predefined standards or best practices. A configuration review can help to identify and remediate any deviations, inconsistencies, or misconfigurations that may expose the application servers to unauthorized access, exploitation, or compromise<sup>6</sup>. A configuration review can also help to ensure compliance with security policies and regulations, as well as enhance the performance and availability of application servers. The other options are less effective or incorrect because:

- ? A. Improving the change management process is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While improving the change management process may help to prevent future inconsistencies or misconfigurations in application server settings, it does not ensure that the existing ones are detected and corrected.
- ? B. Establishing security metrics is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While establishing security metrics may help to measure and monitor the security performance and posture of application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected.
- ? C. Performing a penetration test is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While performing a penetration test may help to simulate and evaluate the impact of an attack on application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected. References: Configuring system to use application server security - IBM, Application Security Risk: Assessment and Modeling - ISACA, Five Key Components of an Application Security Program - ISACA, ISACA Practitioner Guidelines for Auditors - SSH, SCADA Cybersecurity Framework - ISACA

**NEW QUESTION 41**

- (Topic 3)

A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items to the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

- A. Separate authorization for input of transactions
- B. Statistical sampling of adjustment transactions
- C. Unscheduled audits of lost stock lines
- D. An edit check for the validity of the inventory transaction

**Answer:** A

**Explanation:**

Separate authorization for input of transactions. This control would have best prevented this type of fraud in a retail environment by ensuring that the warehouse employee who handles the inventory items does not have the authority to enter adjustments to the inventory system. This would create a segregation of duties that would reduce the risk of collusion and concealment of theft.

The other options are not as effective as option A in preventing this type of fraud. Option B, statistical sampling of adjustment transactions, is a detective control that may help identify fraudulent transactions after they have occurred, but it does not prevent them from happening in the first place. Option C, unscheduled audits of lost stock lines, is also a detective control that may reveal discrepancies between the physical and recorded inventory, but it does not address the root cause of the fraud. Option D, an edit check for the validity of the inventory transaction, is a preventive control that may help verify the accuracy and completeness of the transaction data, but it does not prevent unauthorized or fraudulent adjustments.

References:

- ? ISACA, CISA Review Manual, 27th Edition, 2019
- ? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
- ? Different Types of Inventory Fraud and How to Prevent Them1
- ? 6 Ways to Prevent Inventory Fraud in Your Business2

**NEW QUESTION 45**

- (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 47**

- (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 51**

- (Topic 3)

What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

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

**Answer:** D

**Explanation:**

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 53**

- (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 58**

- (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 60**

- (Topic 3)

Which of the following is MOST important to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition?

- A. Role-based access control policies
- B. Types of data that can be uploaded to the platform
- C. Processes for on-boarding and off-boarding users to the platform
- D. Processes for reviewing administrator activity

**Answer:** B

**Explanation:**

The most important thing to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization's policies and standards for data protection<sup>1</sup>.

The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired<sup>2</sup>. Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is acquired<sup>3</sup>. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established and performed after the platform is acquired<sup>4</sup>.

References:

- ? Cloud Messaging and Collaboration Services - Maryland.gov DoIT4
- ? MessageBird acquires real-time notifications and in-app messaging platform Pusher for \$35M | TechCrunch2
- ? Symphony to lead financial market communications with the acquisition of Cloud9 Technologies3
- ? Cloud messaging and collaboration | Sumo Logic

**NEW QUESTION 64**

- (Topic 3)

Which of the following is the PRIMARY advantage of using visualization technology for corporate applications?

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

**Answer: B**

**Explanation:**

Visualization technology is the use of software and hardware to create graphical representations of data, such as charts, graphs, maps, images, etc. Visualization technology can help users to understand, analyze, and communicate complex and large amounts of data in an intuitive and engaging way1.

One of the primary advantages of using visualization technology for corporate applications is that it can improve the utilization of resources, such as time, money, human capital, and physical assets. Some of the ways that visualization technology can achieve this are:

? Visualization technology can help users to quickly and easily explore, filter, and interact with data, reducing the need for manual data processing and analysis1. This can save time and effort for both data producers and consumers, and allow them to focus on more value-added tasks.

? Visualization technology can help users to discover patterns, trends, outliers, correlations, and causations in data that may otherwise be hidden or overlooked in traditional reports or tables1. This can enable users to make better and faster decisions based on data-driven insights, and optimize their strategies and actions accordingly.

? Visualization technology can help users to communicate and share data more effectively and persuasively with different audiences, such as customers, partners, investors, regulators, etc1. This can enhance the reputation and credibility of the organization, and foster collaboration and innovation among stakeholders.

? Visualization technology can help users to monitor and measure the performance and impact of their activities, products, services, or processes1. This can help users to identify problems or opportunities for improvement, and adjust their plans or actions accordingly.

? Visualization technology can help users to create engaging and interactive experiences for their customers or end-users1. This can increase customer satisfaction and loyalty, and generate more revenue or value for the organization.

Therefore, using visualization technology for corporate applications can help organizations to better utilize their resources and achieve their goals.

References:

- ? ISACA, CISA Review Manual, 27th Edition, 2019
- ? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
- ? TechRadar Blog, Best data visualization tools of 20232
- ? IBM Blog, What is Data Visualization?3
- ? TDWI Blog, Data Visualization Technology4
- ? Tableau Blog, What are the advantages and disadvantages of data visualization?

**NEW QUESTION 68**

- (Topic 3)

An IS auditor assessing the controls within a newly implemented call center would First

- A. gather information from the customers regarding response times and quality of service.
- B. review the manual and automated controls in the call center.
- C. test the technical infrastructure at the call center.
- D. evaluate the operational risk associated with the call center.

**Answer: D**

**Explanation:**

The first step in assessing the controls within a newly implemented call center is to evaluate the operational risk associated with the call center. This will help the IS auditor to identify the potential threats, vulnerabilities, and impacts that could affect the call center's objectives, performance, and availability. The evaluation of operational risk will also provide a basis for determining the scope, objectives, and approach of the audit. The other options are possible audit procedures, but they are not the first step in the audit process. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

**NEW QUESTION 71**

- (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 requirements<sup>3</sup>. The lack of data model documentation may also increase the risk of errors, inconsistencies, and inefficiencies in the data and the application performance<sup>2</sup>.

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 organization<sup>4</sup>. 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 collaboration<sup>5</sup>. 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 | Informatica<sup>1</sup>
- ? Data Modeling Best Practices: Documentation | erwin<sup>2</sup>
- ? Data Model Documentation - an overview | ScienceDirect Topics<sup>3</sup>
- ? Outsourcing App Development Pros and Cons – Droids On Roids<sup>4</sup>
- ? 8 Risks of Software Development Outsourcing & Their Solutions - Acropolisium<sup>5</sup>
- ? Software Training Plan: How to Create One for Your Business - Elinext

#### NEW QUESTION 75

- (Topic 3)

Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

- A. Customer service complaints
- B. Automated monitoring of logs
- C. Server crashes
- D. Penetration testing

**Answer: B**

#### Explanation:

The best way to detect that a distributed denial of service (DDoS) attack is occurring is to use automated monitoring of logs. A DDoS attack disrupts the operations of a server, service, or network by flooding it with unwanted Internet traffic<sup>2</sup>. Automated monitoring of logs can help pinpoint potential DDoS attacks by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and alerting administrators or security teams of any anomalies or malicious requests, protocols, or IP blocks<sup>3</sup>. Automated monitoring of logs can also help identify the source, type, and impact of the DDoS attack, and provide evidence for further investigation or mitigation.

The other options are not as effective as automated monitoring of logs for detecting DDoS attacks. Customer service complaints are an indirect and delayed indicator of a DDoS attack, as they rely on users reporting problems with accessing a website or service. Customer service complaints may also be caused by other factors unrelated to DDoS attacks, such as server errors or network issues. Server crashes are an extreme and undesirable indicator of a DDoS attack, as they indicate that the server has already been overwhelmed by the attack and has stopped functioning. Server crashes may also result in data loss or corruption, service disruption, or reputational damage. Penetration testing is a proactive and preventive measure for assessing the security posture of a system or network, but it does not detect ongoing DDoS attacks. Penetration testing may involve simulating DDoS attacks to test the resilience or vulnerability of a system or network, but it does not monitor real-time traffic or identify actual attackers.

References:

- ? ISACA CISA Review Manual 27th Edition (2019), page 254
- ? How to prevent DDoS attacks | Methods and tools | Cloudflare<sup>2</sup>
- ? Understanding Denial-of-Service Attacks | CISA<sup>3</sup>

#### NEW QUESTION 79

- (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 Subscription<sup>2</sup>

#### NEW QUESTION 83

- (Topic 3)

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

- A. Assign the security risk analysis to a specially trained member of the project management office.
- B. Deploy changes in a controlled environment and observe for security defects.
- C. Include a mandatory step to analyze the security impact when making changes.
- D. Mandate that the change analyses are documented in a standard format.

**Answer: C**

**Explanation:**

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

**NEW QUESTION 85**

- (Topic 3)

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 86**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 91**

- (Topic 3)

Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

- A. Prepare detailed plans for each business function.
- B. Involve staff at all levels in periodic paper walk-through exercises.
- C. Regularly update business impact assessments.
- D. Make senior managers responsible for their plan sections.

**Answer:** B

**Explanation:**

The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies1.

The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities2. Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks2. Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other2.

References:

? Best Practice Guide: Business Continuity Planning (BCP)3

? Best Practices for Creating a Business Continuity Plan1

? Business Continuity Plan Best Practices

**NEW QUESTION 94**

- (Topic 3)

The PRIMARY objective of value delivery in reference to IT governance is to:

- A. promote best practices
- B. increase efficiency.
- C. optimize investments.

D. ensure compliance.

**Answer: C**

**Explanation:**

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 98**

- (Topic 3)

Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's disaster recovery plan (DRP)?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 102**

- (Topic 2)

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 107**

- (Topic 2)

What is the Most critical finding when reviewing an organization's information security management?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 111**

- (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 114**

- (Topic 2)

Which of the following documents should specify roles and responsibilities within an IT audit organization?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 119**

- (Topic 2)

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

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

**Answer: D**

**Explanation:**

The best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet. An IDS is a device or software that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. By placing an IDS between the firewall and the Internet, the IS auditor can enhance the security of the network perimeter and detect any attack attempts that the firewall was unable to recognize.

The other options are not as effective as placing an IDS between the firewall and the Internet:

? Placing an IDS between the firewall and the organization's web server would not protect the web server from external attacks that bypass the firewall. The web server should be placed in a demilitarized zone (DMZ), which is a separate network segment that isolates public-facing servers from the internal network.

? Placing an IDS between the firewall and the demilitarized zone (DMZ) would not protect the DMZ from external attacks that bypass the firewall. The DMZ should be protected by two firewalls, one facing the Internet and one facing the internal network, with an IDS monitoring both sides of each firewall.

? Placing an IDS between the firewall and the organization's network would not protect the organization's network from external attacks that bypass the firewall. The organization's network should be protected by a firewall that blocks unauthorized traffic from entering or leaving the network, with an IDS monitoring both sides of the firewall.

**NEW QUESTION 123**

- (Topic 2)

Which of the following BEST protects an organization's proprietary code during a joint-development activity involving a third party?

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

**Answer: B**

**Explanation:**

A nondisclosure agreement (NDA) is the best way to protect an organization's proprietary code during a joint-development activity involving a third party. An NDA is a legal contract that binds the parties involved in a joint-development activity to keep confidential any information, data or materials that are shared or exchanged during the activity. An NDA specifies what constitutes confidential information, how it can be used, disclosed or protected, how long it remains confidential, what are the exceptions and remedies for breach of confidentiality, and other terms and conditions. An NDA can help to protect an organization's proprietary code from being copied, modified, distributed or exploited by unauthorized parties without its consent or knowledge. The other options are not as effective as option B, as they do not address confidentiality issues specifically. A statement of work (SOW) is a document that defines the scope, objectives, deliverables, tasks, roles,

responsibilities, timelines and costs of a joint-development activity, but it does not cover confidentiality issues explicitly. A service level agreement (SLA) is a document that defines the quality, performance and availability standards and metrics for a service provided by one party to another party in a joint-development activity, but it does not cover confidentiality issues explicitly. A privacy agreement is a document that defines how personal information collected from customers or users is collected, used, disclosed and protected by one party or both parties in a joint-development activity, but it does not cover confidentiality issues related to proprietary code. References: CISA Review Manual (Digital Version) , Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.2: Project Management Practices.

#### NEW QUESTION 125

- (Topic 2)

An organization has assigned two new IS auditors to audit a new system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which of the following is MOST important to meet the IS audit standard for proficiency?

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

**Answer: C**

#### Explanation:

Team member assignments based on individual competencies is the most important factor to meet the IS audit standard for proficiency. Proficiency is the ability to apply knowledge, skills and experience to perform audit tasks effectively and efficiently. The IS audit standard for proficiency requires that IS auditors must possess the knowledge, skills and discipline to perform audit tasks in accordance with applicable standards, guidelines and procedures. Team member assignments based on individual competencies is a way to ensure that each IS auditor is assigned to audit tasks that match their level of proficiency, and that the audit team as a whole has sufficient and appropriate proficiency to conduct the audit. The other options are not as important as option C, as they do not ensure that the IS auditors have the required proficiency to perform audit tasks. Having a globally recognized audit certification is a way to demonstrate proficiency in IS auditing, but it does not guarantee that the IS auditor has the specific knowledge, skills and experience needed for a particular audit task or system. Technical co-sourcing is a way to supplement the proficiency of the IS audit team by hiring external experts or consultants to perform certain audit tasks or functions, but it does not replace the need for internal IS auditors to have adequate proficiency. Having a supervisor review the new auditors' work is a way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

#### NEW QUESTION 126

- (Topic 2)

Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 128

- (Topic 2)

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

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

**Answer: A**

#### Explanation:

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

inconsistencies.

#### NEW QUESTION 129

- (Topic 2)

Which of the following is the BEST indicator of the effectiveness of an organization's incident response program?

- A. Number of successful penetration tests
- B. Percentage of protected business applications
- C. Financial impact per security event
- D. Number of security vulnerability patches

**Answer: C**

#### Explanation:

The best indicator of the effectiveness of an organization's incident response program is the financial impact per security event. This metric measures the direct and indirect costs associated with security incidents, such as loss of revenue, reputation damage, legal fees, recovery expenses, and fines. By reducing the financial impact per security event, the organization can demonstrate that its incident response program is effective in mitigating the consequences of security breaches and restoring normal operations as quickly as possible. Number of successful penetration tests, percentage of protected business applications, and number of security vulnerability patches are indicators of the security posture of the organization, but they do not reflect the effectiveness of the incident response program. References: ISACA Journal Article: Measuring Incident Response Effectiveness

#### NEW QUESTION 133

- (Topic 2)

Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 135

- (Topic 2)

The waterfall life cycle model of software development is BEST suited for which of the following situations?

- A. The protect requirements are well 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 136

- (Topic 2)

The IS quality assurance (QA) group is responsible for:

- A. ensuring that program changes adhere to established standards.
- B. designing procedures to protect data against accidental disclosure.
- C. ensuring that the output received from system processing is complete.
- D. monitoring the execution of computer processing tasks.

**Answer: A**

**Explanation:**

The IS quality assurance (QA) group is responsible for ensuring that program changes adhere to established standards. Program changes are modifications made to software applications or systems to fix errors, improve performance, add functionality, or meet changing requirements. Program changes should follow established standards for documentation, authorization, testing, implementation, and review. The IS QA group is responsible for verifying that program changes comply with these standards and meet the expected quality criteria. Designing procedures to protect data against accidental disclosure; ensuring that the output received from system processing is complete; and monitoring the execution of computer processing tasks are not responsibilities of the IS QA group. References: [ISACA CISA Review Manual 27th Edition], page 304.

**NEW QUESTION 140**

- (Topic 2)

Which of the following BEST Indicates that an incident management process is effective?

- A. Decreased time for incident resolution
- B. Increased number of incidents reviewed by IT management
- C. Decreased number of calls to the help desk
- D. Increased number of reported critical incidents

**Answer: A**

**Explanation:**

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

**NEW QUESTION 144**

- (Topic 2)

An IS auditor is reviewing a recent security incident and is seeking information about the approval of a recent modification to a database system's security settings. Where would the auditor MOST likely find this information?

- A. System event correlation report
- B. Database log
- C. Change log
- D. Security incident and event management (SIEM) report

**Answer: C**

**Explanation:**

A change log is a record of all changes made to a system or application, including the date, time, description, and approval of each change. A change log can help an IS auditor to trace the source and authorization of a modification to a system's security settings. A system event correlation report is a tool that analyzes data from multiple sources to identify patterns and anomalies that indicate potential security incidents. A database log is a record of all transactions and activities performed on a database, such as queries, updates, and backups. A security incident and event management (SIEM) report is a tool that collects, analyzes, and reports on data from various sources to detect and respond to security incidents.

**NEW QUESTION 149**

- (Topic 2)

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

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

**Answer: B**

**Explanation:**

This is the most effective way for the organization to improve its data classification processes and procedures, because data owners are the ones who are responsible for assigning the appropriate level of classification to the data they create, collect, or manage. Data owners should be aware of the data classification policy, the criteria for each level of classification, and the implications of misclassification. IT security staff can provide tailored training for data owners based on their roles, functions, and types of data they handle.

The other options are not as effective as having IT security staff conduct targeted training for data owners:

? Use automatic document classification based on content. This is a possible option, but it may not be feasible or accurate for a small organization. Automatic document classification is a process that uses artificial intelligence or machine learning to analyze the content of a document and assign a class label based on predefined rules or models. However, this process may require a lot of resources, expertise, and maintenance, and it may not capture all the nuances and context of the data. The IS auditor should also verify the reliability and validity of the automatic document classification system.

? Publish the data classification policy on the corporate web portal. This is a good practice, but it is not enough to improve the data classification situation. Publishing the data classification policy on the corporate web portal can increase the visibility and accessibility of the policy, but it does not ensure that data owners will read, understand, and follow it. The IS auditor should also monitor and enforce the compliance with the policy.

? Conduct awareness presentations and seminars for information classification policies. This is a useful measure, but it is not the most effective one. Conducting awareness presentations and seminars can raise the general awareness and knowledge of information classification policies among all employees, but it may not address the specific needs and challenges of data owners. The IS auditor should also provide more in-depth and practical training for data owners.

**NEW QUESTION 152**

- (Topic 2)

When auditing the alignment of IT to the business strategy, it is MOST Important for the IS auditor to:

- A. compare the organization's strategic plan against industry best practice.

- B. interview senior managers for their opinion of the IT function.
- C. ensure an IT steering committee is appointed to monitor new IT projects.
- D. evaluate deliverables of new IT initiatives against planned business services.

**Answer:** D

**Explanation:**

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

**NEW QUESTION 156**

- (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 157**

- (Topic 2)

A project team has decided to switch to an agile approach to develop a replacement for an existing business application. Which of the following should an IS auditor do FIRST to ensure the effectiveness of the protect audit?

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

**Answer:** C

**Explanation:**

Understanding the specific agile methodology that will be followed is the first step that an IS auditor should do to ensure the effectiveness of the project audit. An IS auditor should familiarize themselves with the agile approach, principles, practices, and tools that will be used by the project team, as well as the roles and responsibilities of the project stakeholders. This will help the IS auditor to identify and assess the relevant risks and controls for the project audit. The other options are not the first steps that an IS auditor should do, but rather possible subsequent actions that may depend on the specific agile methodology. References:

? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.21

? CISA Review Questions, Answers & Explanations Database, Question ID 211

**NEW QUESTION 159**

- (Topic 2)

In order to be useful, a key performance indicator (KPI) MUST

- A. be approved by management.
- B. be measurable in percentages.
- C. be changed frequently to reflect organizational strategy.
- D. have a target value.

**Answer:** D

**Explanation:**

A key performance indicator (KPI) is a quantifiable measure of performance over time for a specific objective<sup>1</sup>. KPIs help organizations and teams track their progress and achievements towards their strategic goals. To be useful, a KPI must have a target value, which is the desired level of performance or outcome that the organization or team aims to achieve. A target value provides a clear direction and a benchmark for measuring success or failure. Without a target value, a KPI is meaningless, as it does not indicate whether the performance is good or bad, or how far or close the organization or team is from reaching their objective.

**NEW QUESTION 164**

- (Topic 2)

Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm for potential software vulnerabilities?

- A. Guest operating systems are updated monthly
- B. The hypervisor is updated quarterly.

- C. A variety of guest operating systems operate on one virtual server
- D. Antivirus software has been implemented on the guest operating system only.

**Answer:** D

**Explanation:**

Antivirus software has been implemented on the guest operating system only is the observation that an IS auditor would consider the greatest risk when conducting an audit of a virtual server farm for potential software vulnerabilities. A virtual server farm is a collection of servers that run multiple virtual machines (VMs) on a single physical host using a software layer called a hypervisor. A guest operating system is the operating system installed on each VM. Antivirus software is a software program that detects and removes malicious software from a computer system. If antivirus software has been implemented on the guest operating system only, it means that the hypervisor and the host operating system are not protected from malware attacks, which could compromise the security and availability of all VMs running on the same host. Therefore, antivirus software should be implemented on both the guest and host operating systems as well as on the hypervisor. References: CISA Review Manual, 27th Edition, page 378

**NEW QUESTION 169**

- (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 174**

- (Topic 2)

Which of the following findings from an IT governance review should be of GREATEST concern?

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

**Answer:** C

**Explanation:**

IT value analysis has not been completed is a finding from an IT governance review that should be of greatest concern. IT value analysis is a process of measuring and demonstrating the contribution of IT to the organization's goals and objectives. An IS auditor should be concerned about the lack of IT value analysis, as it may indicate that the IT investments and resources are not aligned with the business needs and expectations, or that the IT performance and outcomes are not monitored and evaluated. The other options are less critical findings that may not have a significant impact on the IT governance. References:

? CISA Review Manual (Digital Version), Chapter 5, Section 5.11

? CISA Review Questions, Answers & Explanations Database, Question ID 218

**NEW QUESTION 178**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

data inputs when moving from one DBMS to another can help ensure the integrity of the system throughout the change by reducing errors or inconsistencies in data input or collection.

#### NEW QUESTION 182

- (Topic 2)

When testing the adequacy of tape backup procedures, which step BEST verifies that regularly scheduled Backups are timely and run to completion?

- A. Observing the execution of a daily backup run
- B. Evaluating the backup policies and procedures
- C. Interviewing key personnel evolved In the backup process
- D. Reviewing a sample of system-generated backup logs

**Answer:** D

#### Explanation:

Reviewing a sample of system-generated backup logs is the best step to verify that regularly scheduled backups are timely and run to completion. Backup logs are records that document the details and results of backup operations, such as the date, time, duration, status, errors, and exceptions. By reviewing a sample of backup logs, the IS auditor can check whether the backups are performed according to the schedule and whether they are completed successfully or not. The other steps do not provide as much evidence or assurance as reviewing backup logs, as they do not show the actual outcome or performance of backup operations. References: CISA Review Manual, 27th Edition, page 247

#### NEW QUESTION 183

- (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 186

- (Topic 2)

During a follow-up audit, it was found that a complex security vulnerability of low risk was not resolved within the agreed-upon timeframe. IT has stated that the system with the identified vulnerability is being replaced and is expected to be fully functional in two months Which of the following is the BEST course of action?

- A. Require documentation that the finding will be addressed within the new system
- B. Schedule a meeting to discuss the issue with senior management
- C. Perform an ad hoc audit to determine if the vulnerability has been exploited
- D. Recommend the finding be resolved prior to implementing the new system

**Answer:** A

#### Explanation:

Requiring documentation that the finding will be addressed within the new system is the best course of action for a follow-up audit. An IS auditor should obtain evidence that the complex security vulnerability of low risk will be resolved in the new system and that there is a reasonable timeline for its implementation. The other options are not appropriate courses of action, as they may be too costly, time-consuming, or impractical for a low-risk finding. References:

? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31

? CISA Review Questions, Answers & Explanations Database, Question ID 209

#### NEW QUESTION 191

- (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 195

- (Topic 2)

To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

- A. Review IT staff job descriptions for alignment
- B. Develop quarterly training for each IT staff member.
- C. Identify required IT skill sets that support key business processes
- D. Include strategic objectives in IT staff performance objectives

**Answer: C**

#### Explanation:

Identifying required IT skill sets that support key business processes is the first step to enable the alignment of IT staff development plans with IT strategy. An IT strategy is a plan that defines how IT will support the organization's goals and objectives. Identifying required IT skill sets means determining the knowledge, abilities, and competencies that IT staff need to perform their roles and responsibilities effectively and efficiently. This can help to align IT staff development plans with IT strategy, as well as to identify and address any skill gaps or needs within the IT workforce. The other options are not the first steps to enable alignment, but rather possible subsequent actions that may depend on the required IT skill sets. References:

? CISA Review Manual (Digital Version), Chapter 5, Section 5.11

? CISA Review Questions, Answers & Explanations Database, Question ID 229

### NEW QUESTION 197

- (Topic 2)

When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the.

- A. architecture and cloud environment of the system.
- B. business process supported by the system.
- C. policies and procedures of the business area being audited.
- D. availability reports associated with the cloud-based system.

**Answer: B**

#### Explanation:

The business process supported by the system is the most important factor for an IS auditor to understand when planning an audit to assess application controls of a cloud-based system. An IS auditor should have a clear understanding of the business objectives, requirements, and risks of the process, as well as the expected outputs and outcomes of the system. This will help the IS auditor to determine the scope, objectives, and criteria of the audit, as well as to identify and evaluate the key application controls that ensure the effectiveness, efficiency, and reliability of the process. The other options are less important factors that may provide additional information or context for the audit, but not its primary focus. References:

? CISA Review Manual (Digital Version), Chapter 5, Section 5.31

? CISA Review Questions, Answers & Explanations Database, Question ID 212

### NEW QUESTION 198

- (Topic 2)

Which of the following is the MOST important activity in the data classification process?

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

**Answer: C**

#### Explanation:

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

### NEW QUESTION 200

- (Topic 2)

Stress testing should ideally be carried out under a:

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

**Answer: A**

#### Explanation:

Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not

suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:

? CISA Review Manual, 27th Edition, pages 471-4721

? CISA Review Questions, Answers & Explanations Database, Question ID: 261

#### **NEW QUESTION 201**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **CISA Practice Exam Features:**

- \* CISA Questions and Answers Updated Frequently
- \* CISA Practice Questions Verified by Expert Senior Certified Staff
- \* CISA Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* CISA Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CISA Practice Test Here](#)**