

# Isaca

## Exam Questions CISA

Isaca CISA



### NEW QUESTION 1

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.1

### NEW QUESTION 2

- (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 3

- (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 4

- (Topic 3)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 5

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources, procedures, communication plans, and backup 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 6

- (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 7

- (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 8

- (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 9

- (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 10

- (Topic 3)

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

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

**Answer: B**

#### Explanation:

When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements. The security criteria should define the level of confidentiality, integrity, and availability for each data classification, as well as the corresponding controls such as access control, rights management, and cryptographic 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 10

- (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 15

- (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 20

- (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 21

- (Topic 3)

The PRIMARY benefit of information asset classification is that it:

- A. prevents loss of assets.
- B. helps to align organizational objectives.

- C. facilitates budgeting accuracy.
- D. enables risk management decisions.

**Answer:** D

**Explanation:**

The primary benefit of information asset classification is that it enables risk management decisions. Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 300

**NEW QUESTION 23**

- (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 27**

- (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 32**

- (Topic 3)

An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

- A. reclassify the data to a lower level of confidentiality
- B. require the business owner to conduct regular access reviews.
- C. implement a strong password schema for users.
- D. recommend corrective actions to be taken by the security administrator.

**Answer: B**

**Explanation:**

The best recommendation for an IS auditor who finds that one employee has unauthorized access to confidential data is to require the business owner to conduct regular access reviews. Access reviews are periodic assessments of user access rights and permissions to ensure that they are appropriate, necessary, and aligned with the business needs and objectives. Access reviews help to identify and remediate any unauthorized, excessive, or obsolete access that could pose a security risk or violate compliance requirements. The business owner is responsible for defining and approving the access requirements for their data and ensuring that they are enforced and monitored. References:

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 34**

- (Topic 3)

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

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

**Answer: A**

**Explanation:**

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 37**

- (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 Work1

? Protecting your personal information and privacy on a company phone2

? Mobile Devices and Protected Health Information (PHI)3

? Using your personal phone for work? Here's how to separate your apps and data4

? 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

**NEW QUESTION 38**

- (Topic 3)

Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks?

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

**Answer: A**

**Explanation:**

The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic

human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures<sup>12</sup>. Without a proper documentation of the end-to-end process, the organization may face challenges in designing, developing, testing, deploying, and monitoring the RPA solution<sup>3</sup>. References:

1: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211  
 2: CISA Online Review Course, Module 4: Information Systems Operations and Business Resilience, Lesson 4.2: IT Service Delivery and Support  
 3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

#### NEW QUESTION 40

- (Topic 3)

A post-implementation review was conducted by issuing a survey to users. Which of the following should be of GREATEST concern to an IS auditor?

- A. The survey results were not presented in detail to management.
- B. The survey questions did not address the scope of the business case.
- C. The survey form template did not allow additional feedback to be provided.
- D. The survey was issued to employees a month after implementation.

**Answer: B**

#### Explanation:

The greatest concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users is that the survey questions did not address the scope of the business case. A post-implementation review is a process of evaluating the outcomes and benefits of a project after it has been completed and implemented. A post-implementation review can help to assess whether the project met its objectives, delivered its expected value, and satisfied its stakeholders<sup>1</sup>. A survey is a method of collecting feedback and opinions from users or other stakeholders about their experience and satisfaction with the project. A survey can help to measure the user acceptance, usability, and functionality of the project deliverables<sup>2</sup>. A business case is a document that justifies the need for a project based on its expected benefits, costs, risks, and alternatives. A business case defines the scope, objectives, and requirements of the project and provides a basis for its approval and initiation<sup>3</sup>. Therefore, an IS auditor should be concerned if the survey questions did not address the scope of the business case, as it may indicate that the post-implementation review was not comprehensive, relevant, or aligned with the project goals. The other options are less concerning or incorrect because:

- ? A. The survey results were not presented in detail to management is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a communication or reporting issue than an audit issue. While presenting the survey results in detail to management may help to inform them about the project performance and outcomes, it does not affect the validity or quality of the post-implementation review itself.
- ? C. The survey form template did not allow additional feedback to be provided is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a design or format issue than an audit issue. While allowing additional feedback to be provided may help to capture more insights or suggestions from users, it does not affect the validity or quality of the post-implementation review itself.
- ? D. The survey was issued to employees a month after implementation is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a timing or scheduling issue than an audit issue. While issuing the survey to employees sooner after implementation may help to collect more accurate and timely feedback from users, it does not affect the validity or quality of the post-implementation review itself. References: Post Implementation Review - ISACA, Survey - ISACA, Business Case - ISACA

#### NEW QUESTION 42

- (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 - ISACA<sup>1</sup>
- ? Incident Response: How to Identify and Fix Security Weaknesses

#### NEW QUESTION 43

- (Topic 3)

Which of the following presents the GREATEST challenge to the alignment of business and IT?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 48**

- (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 52**

- (Topic 3)

An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that

- A. security parameters are set in accordance with the manufacturer's standards.
- B. a detailed business case was formally approved prior to the purchase.
- C. security parameters are set in accordance with the organization's policies.
- D. the procurement project invited tenders from at least three different suppliers.

**Answer: C**

**Explanation:**

The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies. Security parameters are settings or options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization's policies are documents that define the security goals, requirements, standards, and guidelines for the organization's information systems. An IS auditor should verify that security parameters are set in accordance with the organization's policies to ensure that the new server complies with the organization's security expectations and regulations. The other options are less important or incorrect because:

? A. Security parameters should not be set in accordance with the manufacturer's standards alone, as they may not reflect the organization's specific security needs and environment. The manufacturer's standards are general recommendations or best practices for configuring the server's security parameters based on common scenarios and threats. An IS auditor should compare the manufacturer's standards with the organization's policies and identify any gaps or conflicts that need to be resolved.

? B. A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.

? D. The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization. References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA], [Business Case- ISACA], [Tender - ISACA], [Procurement Management - ISACA]

**NEW QUESTION 57**

- (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 tables<sup>1</sup>. 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, etc<sup>1</sup>. 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 processes<sup>1</sup>. 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-users<sup>1</sup>. 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 2023<sup>2</sup>

? IBM Blog, What is Data Visualization?<sup>3</sup>

? TDWI Blog, Data Visualization Technology<sup>4</sup>

? Tableau Blog, What are the advantages and disadvantages of data visualization?

### NEW QUESTION 61

- (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 66

- (Topic 3)

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

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

**Answer: B**

#### Explanation:

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

### NEW QUESTION 70

- (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 | Cloudflare2
- ? Understanding Denial-of-Service Attacks | CISA3

**NEW QUESTION 72**

- (Topic 3)

Which of the following is the BEST way to enforce the principle of least privilege on a server containing data with different security classifications?

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

**Answer: C**

**Explanation:**

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

References:

- ? CISA Review Manual (Digital Version)
- ? CISA Questions, Answers & Explanations Database

**NEW QUESTION 77**

- (Topic 3)

Which of the following would be MOST useful when analyzing computer performance?

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

**Answer: A**

**Explanation:**

Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.

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

References:

- ? What is Computer Performance?
- ? How to Measure Computer Performance

**NEW QUESTION 82**

- (Topic 3)

Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

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

**Answer: B**

**Explanation:**

The most important consideration for an IS auditor when assessing the adequacy of an organization's information security policy is the business objectives. An information security policy is a document that defines the organization's approach to protecting its information assets from internal and external threats. It should align with the organization's mission, vision, values, and goals, and support its business processes and functions<sup>1</sup>. An information security policy should also be focused on the business needs and requirements of the organization, rather than on technical details or specific solutions<sup>2</sup>. The other options are not as important as the business objectives, because they do not directly reflect the organization's purpose and direction. IT steering committee minutes are records of the discussions and decisions made by a group of senior executives who oversee the IT strategy and governance of the organization. They may provide some insights into the information security policy, but they are not sufficient to evaluate its adequacy<sup>3</sup>. Alignment with the IT tactical plan is a measure of how well the information security policy supports the short-term actions and projects that implement the IT strategy. However, the IT tactical plan itself should be aligned with the business objectives, and not vice versa<sup>4</sup>. Compliance with industry best practice is a desirable quality of an information security policy, but it is not a guarantee of its effectiveness or suitability for the organization. Industry best practices are general guidelines or recommendations that may not apply to every organization or situation. An information security policy should be customized and tailored to the specific context and needs of the organization. References:

- ? The 12 Elements of an Information Security Policy | Exabeam<sup>1</sup>
- ? 11 Key Elements of an Information Security Policy | Egnyte<sup>2</sup>
- ? What is an IT steering committee? Definition, roles & responsibilities ...<sup>3</sup>
- ? What is IT Strategy? Definition, Components & Best Practices | BMC ...<sup>4</sup>
- ? IT Security Policy: Key Components & Best Practices for Every Business

### NEW QUESTION 87

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

? CISA Review Manual, 27th Edition, page 2301

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

### NEW QUESTION 92

- (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 93

- (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 96

- (Topic 3)

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

- A. A formal request for proposal (RFP) process
- B. Business case development procedures
- C. An information asset acquisition policy
- D. Asset life cycle management.

**Answer: D**

#### Explanation:

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

The other options are not as effective as asset life cycle management for preventing unused applications. A formal request for proposal (RFP) process is a method of soliciting bids from potential vendors or suppliers for a project or service. A RFP process can help select the best application for a specific requirement, but it does not ensure that the application will be used or maintained throughout its lifecycle. Business case development procedures are a set of steps that involve

defining the problem, analyzing the alternatives, and proposing a solution for a project or initiative. Business case development procedures can help justify the need and value of an application, but they do not guarantee that the application will be utilized or supported after its implementation. An information asset acquisition policy is a document that outlines the rules and standards for acquiring information assets such as applications. An information asset acquisition policy can help ensure that the applications are acquired in a consistent and compliant manner, but it does not address how the applications will be managed or disposed of after their acquisition.

#### NEW QUESTION 99

- (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 101

- (Topic 3)

Which of the following issues associated with a data center's closed-circuit television (CCTV) surveillance cameras should be of MOST concern to an IS auditor?

- A. CCTV recordings are not regularly reviewed.
- B. CCTV cameras are not installed in break rooms
- C. CCTV records are deleted after one year.
- D. CCTV footage is not recorded 24 x 7.

**Answer: A**

#### Explanation:

The most concerning issue associated with a data center's CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and regulations. If the recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.

The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection. CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel. References:

? ISACA Journal Article: Physical security of a data center<sup>1</sup>

? Data Center Security: Checklist and Best Practices | Kisi<sup>2</sup>

? Video Surveillance Best Practices | Taylored Systems

#### NEW QUESTION 105

- (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 465-466<sup>1</sup>

? CISA Review Questions, Answers & Explanations Database, Question ID: 263

#### NEW QUESTION 109

- (Topic 2)

Which of the following is the BEST reason for an organization to use clustering?

- A. To decrease system response time
- B. To Improve the recovery time objective (RTO)
- C. To facilitate faster backups

D. To improve system resiliency

**Answer: D**

**Explanation:**

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

**NEW QUESTION 113**

- (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 115**

- (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 119**

- (Topic 2)

An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

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

**Answer: C**

**Explanation:**

This should result in a finding because it violates the best practice of setting rules for groups rather than users. According to one of the web search results<sup>1</sup>, using group permissions instead of individual permissions can simplify the management and maintenance of ACLs, reduce the risk of human errors, and ensure consistency and compliance. Individual permissions can create conflicts, confusion, and security gaps in the ACLs. Therefore, the IS auditor should report this as a finding and recommend using group permissions instead.

**NEW QUESTION 122**

- (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 124**

- (Topic 2)

Which of the following is MOST important to verify when determining the completeness of the vulnerability scanning process?

- A. The organization's systems inventory is kept up to date.
- B. Vulnerability scanning results are reported to the CISO.
- C. The organization is using a cloud-hosted scanning tool for Identification of vulnerabilities
- D. Access to the vulnerability scanning tool is periodically reviewed

**Answer: A**

**Explanation:**

The completeness of the vulnerability scanning process depends on the accuracy and currency of the organization's systems inventory, which is a list of all the hardware and software assets that are owned or used by the organization. A complete and up-to-date systems inventory can help ensure that all the systems are identified and scanned for vulnerabilities, and that no system is missed or overlooked. Vulnerability scanning results are reported to the CISO is a good practice for ensuring accountability and visibility of the vulnerability management process, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as reporting does not guarantee that all the systems are scanned. The organization is using a cloud-hosted scanning tool for identification of vulnerabilities is a possible option for conducting vulnerability scanning, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as the type of scanning tool does not affect the scope or coverage of the scanning. Access to the vulnerability scanning tool is periodically reviewed is a critical control for ensuring the security and integrity of the vulnerability scanning tool, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as access review does not ensure that all the systems are scanned.

**NEW QUESTION 128**

- (Topic 2)

The PRIMARY focus of a post-implementation review is to verify that:

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 129**

- (Topic 2)

An internal audit department recently established a quality assurance (QA) program. Which of the following activities is MOST important to include as part of the QA program requirements?

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

**Answer: B**

**Explanation:**

Ongoing monitoring of the audit activities is the most important activity to include as part of the quality assurance (QA) program requirements for an internal audit

department. An IS auditor should perform regular reviews and evaluations of the audit processes, methods, standards, and outcomes to ensure that they comply with the QA program objectives and criteria. This will help to maintain and improve the quality and consistency of the audit services and deliverables. The other options are less important activities to include as part of the QA program requirements, as they may involve long-term resource planning, user satisfaction reports, or feedback from internal audit staff. References:

? CISA Review Manual (Digital Version), Chapter 2, Section 2.61

? CISA Review Questions, Answers & Explanations Database, Question ID 224

#### NEW QUESTION 131

- (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 133

- (Topic 2)

Which of the following is MOST important for an IS auditor to verify when evaluating an organization's firewall?

- A. Logs are being collected in a separate protected host
- B. Automated alerts are being sent when a risk is detected
- C. Insider attacks are being controlled
- D. Access to configuration files is restricted.

**Answer: A**

#### Explanation:

A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can help protect an organization's network and information systems from unauthorized or malicious access, by filtering or blocking unwanted or harmful packets. The most important thing for an IS auditor to verify when evaluating an organization's firewall is that the logs are being collected in a separate protected host. Logs are records of events or activities that occur on a system or network, such as connections, requests, responses, errors, and alerts. Logs can provide valuable information for auditing, monitoring, troubleshooting, and investigating security incidents. However, logs can also be tampered with, deleted, or corrupted by attackers or insiders who want to hide their tracks or evidence of their actions. Therefore, it is essential that logs are stored in a separate host that is isolated and secured from the network and the firewall itself, to prevent unauthorized access or modification of the logs. Automated alerts are being sent when a risk is detected is a good practice for enhancing the security and efficiency of a firewall, but it is not the most important thing for an IS auditor to verify, as alerts may not always be accurate, timely, or actionable. Insider attacks are being controlled is a desirable outcome for a firewall, but it is not the most important thing for an IS auditor to verify, as insider attacks may involve other factors or methods that bypass or compromise the firewall, such as social engineering, credential theft, or physical access. Access to configuration files is restricted is a critical control for ensuring the security and integrity of a firewall, but it is not the most important thing for an IS auditor to verify, as configuration files may not reflect the actual state or performance of the firewall.

#### NEW QUESTION 136

- (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 137

- (Topic 2)

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor's BEST recommendation to facilitate compliance with the regulation?

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

Answer: D

**Explanation:**

The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.

The other options are not as effective as including the requirement in the incident management response plan:

? Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.

? Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.

? Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

**NEW QUESTION 140**

- (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 141**

- (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 142**

- (Topic 2)

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

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

Answer: C

**Explanation:**

Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training. References:

? CISA Review Manual (Digital Version), Chapter 5, Section 5.51

? CISA Review Questions, Answers & Explanations Database, Question ID 228

**NEW QUESTION 147**

- (Topic 2)

Which of the following is the GREATEST risk associated with storing customer data on a web server?

- A. Data availability
- B. Data confidentiality
- C. Data integrity
- D. Data redundancy

**Answer: B**

**Explanation:**

The greatest risk associated with storing customer data on a web server is data confidentiality. Data confidentiality is the property that ensures that data are accessible only to authorized entities or individuals, and protected from unauthorized disclosure or exposure. Storing customer data on a web server poses a high risk to data confidentiality, as web servers are exposed to the internet and may be vulnerable to various types of attacks or breaches that can compromise the security and privacy of customer data, such as hacking, phishing, malware, denial of service (DoS), etc. Customer data may contain sensitive or personal information that can cause harm or damage to customers or the organization if disclosed or exposed, such as identity theft, fraud, reputation loss, legal liability, etc. Data availability is the property that ensures that data are accessible and usable by authorized entities or individuals when needed. Data availability is a risk associated with storing customer data on a web server, as web servers may experience failures or disruptions that can affect the accessibility and usability of customer data, such as hardware faults, network issues, power outages, etc. However, data availability is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data integrity is the property that ensures that data are accurate and consistent, and protected from unauthorized modification or corruption. Data integrity is a risk associated with storing customer data on a web server, as web servers may be subject to attacks or errors that can affect the accuracy and consistency of customer data, such as injection attacks, tampering, replication issues, etc. However, data integrity is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data redundancy is the condition of having duplicate or unnecessary data in a database or system. Data redundancy is not a risk associated with storing customer data on a web server, but rather a result of poor database design or management.

**NEW QUESTION 149**

- (Topic 2)

Which of the following BEST enables the timely identification of risk exposure?

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

**Answer: C**

**Explanation:**

Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References: ISACA CISA Review Manual 27th Edition, page 95.

**NEW QUESTION 150**

- (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 155**

- (Topic 2)

The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

- A. the access control system's log settings.
- B. how the latest system changes were implemented.
- C. the access control system's configuration.
- D. the access rights that have been granted.

**Answer: D**

**Explanation:**

The best way to determine whether programmers have permission to alter data in the production environment is by reviewing the access rights that have been granted. Access rights are permissions or privileges that define what actions or operations a user can perform on an information system or resource. By reviewing

the access rights that have been granted to programmers, an IS auditor can verify whether they have been authorized to modify data in the production environment, which is where live data and applications are stored and executed. The access control system's log settings are parameters that define what events or activities are recorded by the access control system, which is a system that enforces the access rights and policies of an information system or resource. The access control system's log settings are not the best way to determine whether programmers have permission to alter data in the production environment, as they do not indicate what permissions or privileges have been granted to programmers. How the latest system changes were implemented is a process that describes how software updates or modifications are deployed to the production environment. How the latest system changes were implemented is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers. The access control system's configuration is a set of rules or parameters that define how the access control system operates and functions. The access control system's configuration is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers.

#### NEW QUESTION 158

- (Topic 2)

Which of the following business continuity activities prioritizes the recovery of critical functions?

- A. Business continuity plan (BCP) testing
- B. Business impact analysis (BIA)
- C. Disaster recovery plan (DRP) testing
- D. Risk assessment

**Answer: B**

#### Explanation:

A business impact analysis (BIA) is a process that identifies and evaluates the potential effects or consequences of disruptions or disasters on an organization's critical business functions or processes. A BIA can help prioritize the recovery of critical functions by assessing their importance and urgency for the organization's operations, objectives, and stakeholders, and determining their recovery time objectives (RTOs), which are the maximum acceptable time for restoring a function after a disruption. A business continuity plan (BCP) testing is a process that verifies and validates the effectiveness and readiness of a BCP, which is a document that outlines the strategies and procedures for ensuring the continuity of critical business functions in the event of a disruption or disaster. A BCP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are recovered according to the BCP. A disaster recovery plan (DRP) testing is a process that verifies and validates the effectiveness and readiness of a DRP, which is a document that outlines the technical and operational steps for restoring the IT systems and infrastructure that support critical business functions in the event of a disruption or disaster. A DRP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are supported by the IT systems and infrastructure according to the DRP. A risk assessment is a process that identifies and analyzes the potential threats and vulnerabilities that could affect an organization's critical business functions or processes. A risk assessment does not prioritize the recovery of critical functions, but rather estimates their likelihood and impact of being disrupted by various risk scenarios.

#### NEW QUESTION 160

- (Topic 2)

Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 161

- (Topic 2)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 162

- (Topic 2)

An IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer payments. The IS auditor should FIRST

- A. document the exception in an audit report.
- B. review security incident reports.
- C. identify compensating controls.
- D. notify the audit committee.

**Answer: C**

**Explanation:**

The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:

? CISA Review Manual, 27th Edition, pages 295-2961

? CISA Review Questions, Answers & Explanations Database, Question ID: 260

**NEW QUESTION 164**

- (Topic 2)

An IS auditor notes that IT and the business have different opinions on the availability of their application servers. Which of the following should the IS auditor review FIRST in order to understand the problem?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 169**

- (Topic 2)

Which of the following is the MAIN purpose of an information security management system?

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

**Answer: D**

**Explanation:**

The main purpose of an information security management system (ISMS) is to reduce the frequency and impact of information security incidents. An ISMS is a systematic approach to managing information security risks, policies, procedures, and controls within an organization. An ISMS aims to ensure the confidentiality, integrity, and availability of information assets, as well as to comply with relevant laws and regulations. The other options are not the main purpose of an ISMS, but rather some of its possible benefits or components. References:

? CISA Review Manual (Digital Version), Chapter 7, Section 7.11

? CISA Review Questions, Answers & Explanations Database, Question ID 205

**NEW QUESTION 170**

- (Topic 2)

Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

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

**Answer: C**

**NEW QUESTION 174**

- (Topic 2)

The due date of an audit project is approaching, and the audit manager has determined that only 60% of the audit has been completed. Which of the following should the audit manager do FIRST?

- A. Determine where delays have occurred
- B. Assign additional resources to supplement the audit
- C. Escalate to the audit committee
- D. Extend the audit deadline

**Answer: A**

**Explanation:**

The first thing that the audit manager should do when faced with a situation where only 60% of the audit has been completed and the due date is approaching is to determine where delays have occurred. This can help the audit manager to identify and analyze the root causes of the delays, such as unexpected issues, scope changes, resource constraints, communication problems, etc., and evaluate their impact on the audit objectives, scope, quality, and timeline. Based on this analysis, the audit manager can then decide on the best course of action to address the delays and complete the audit successfully. Assigning additional resources to supplement the audit is a possible option for resolving delays in an audit project, but it is not the first thing that the audit manager should do, as it may not be feasible or effective depending on the availability, cost, and suitability of the additional resources. Escalating to the audit committee is a possible option for communicating delays in an audit project and seeking guidance or support from senior management, but it is not the first thing that the audit manager should do, as it may not be necessary or appropriate depending on the severity and urgency of the delays. Extending the audit deadline is a possible option for accommodating delays in an audit project and ensuring sufficient time for completing the audit tasks and activities, but it is not the first thing that the audit manager should do, as it may not be possible or desirable depending on the contractual obligations, stakeholder expectations, and regulatory requirements.

**NEW QUESTION 177**

- (Topic 2)

A manager identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor in this scenario?

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

**Answer: A**

**Explanation:**

A threat actor is an entity or individual that poses a potential harm or danger to an organization's information systems or data. Terminated staff are the threat actors in this scenario, as they are former employees who may still have active privileged accounts that grant them access to sensitive or critical information or resources of the organization. Terminated staff may abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of the information systems or data, either intentionally or unintentionally. Unauthorized access is a threat event or action that occurs when an unauthorized entity or individual gains access to an organization's information systems or data without permission or authorization. Unauthorized access is not a threat actor, but rather a result of a threat actor's activity. Deleted log data is a threat consequence or impact that occurs when log data, which are records of events or activities that occur on an information system or network, are erased or corrupted by a threat actor. Deleted log data can affect the auditability, accountability, and visibility of the information system or network, and prevent detection or investigation of security incidents. Deleted log data is not a threat actor, but rather a result of a threat actor's activity. Hacktivists are threat actors who use hacking techniques to promote a political or social cause or agenda. Hacktivists are not the threat actors in this scenario, as there is no indication that they are involved in this case.

**NEW QUESTION 181**

- (Topic 2)

During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What should the auditor do FIRST?

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

**Answer: A**

**Explanation:**

Asking management why the regulatory changes have not been included is the first thing that an IS auditor should do during the planning stage of a compliance audit. An IS auditor should inquire about the reasons for not updating the inventory of compliance requirements with recent regulatory changes related to managing data risk. This will help the IS auditor to understand whether there is a gap in awareness, communication, or implementation of compliance obligations within the organization. The other options are not the first things that an IS auditor should do, but rather possible subsequent actions that may depend on management's response. References:

? CISA Review Manual (Digital Version), Chapter 2, Section 2.31

? CISA Review Questions, Answers & Explanations Database, Question ID 214

**NEW QUESTION 186**

- (Topic 2)

An IS auditor should ensure that an application's audit trail:

- A. has adequate security.
- B. logs all database records.
- C. Is accessible online
- D. does not impact operational efficiency

**Answer: A**

**Explanation:**

An application's audit trail is a record of all actions or events that occur within or affect an application, such as user activities, system operations, data changes, errors, exceptions, etc. An audit trail can provide evidence and accountability for an application's functionality and performance, and support auditing, monitoring, troubleshooting, and investigation purposes. An IS auditor should ensure that an application's audit trail has adequate security, which means that it is protected from unauthorized access, modification, deletion, or disclosure. Adequate security can help ensure that an audit trail maintains its integrity, reliability, and availability, and prevents tampering or manipulation by attackers or insiders who want to hide their tracks or evidence of their actions. Logging all database records is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as logging all database records may not be necessary or feasible for some applications, and may generate excessive or irrelevant data that can affect the storage or analysis of the audit trail. Is accessible online is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as online accessibility may not be required or desirable for some applications, and may introduce security or privacy risks for the audit trail. Does not impact operational efficiency is a desirable outcome of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as operational efficiency may not be the primary objective or concern of an application's audit trail, and may depend on other factors or trade-offs such as storage capacity, performance speed, or data quality.

### NEW QUESTION 189

- (Topic 2)

During an audit of a multinational bank's disposal process, an IS auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

- A. Backup media are not reviewed before disposal.
- B. Degaussing is used instead of physical shredding.
- C. Backup media are disposed before the end of the retention period
- D. Hardware is not destroyed by a certified vendor.

**Answer: C**

#### Explanation:

During an audit of a multinational bank's disposal process, an IS auditor should be most concerned about backup media being disposed before the end of the retention period. This is because backup media contain sensitive and critical data that may be required for business continuity, legal compliance, or forensic purposes. Disposing backup media prematurely may result in data loss, unavailability, or corruption, which may have severe consequences for the bank's reputation, operations, and security. Backup media not being reviewed before disposal, degaussing being used instead of physical shredding, and hardware not being destroyed by a certified vendor are also findings that may pose some risks to the bank's disposal process, but they are not as critical as backup media being disposed before the end of the retention period. References: ISACA CISA Review Manual 27th Edition, page 302.

### NEW QUESTION 191

- (Topic 2)

Which of the following should an IS auditor consider FIRST when evaluating firewall rules?

- A. The organization's security policy
- B. The number of remote nodes
- C. The firewalls' default settings
- D. The physical location of the firewalls

**Answer: A**

#### Explanation:

This should be the first thing that an IS auditor considers when evaluating firewall rules, because it defines the objectives, standards, and guidelines for securing the organization's network and information assets. The firewall rules should be aligned with the organization's security policy, and reflect the level of risk and protection required for each type of network traffic, system, or data. The IS auditor should compare the firewall rules with the security policy, and identify any discrepancies, gaps, or conflicts that could compromise the security or performance of the network.

The other options are not as important as the organization's security policy when evaluating firewall rules:

? The number of remote nodes. This is a factor that may affect the complexity and scalability of the firewall rules, but it is not a primary consideration for the IS auditor. Remote nodes are devices or systems that connect to the network from outside locations, such as teleworkers, mobile users, or branch offices. The IS auditor should ensure that the firewall rules provide adequate security and access control for remote nodes, but this depends on the organization's security policy and business needs.

? The firewalls' default settings. These are the predefined configurations that come with the firewall devices or software, and that determine how they handle network traffic by default. The IS auditor should review the firewalls' default settings, and verify that they are appropriate and secure for the organization's network environment. However, the firewalls' default settings may not match the organization's security policy or specific requirements, and may need to be customized or overridden by firewall rules.

? The physical location of the firewalls. This is a factor that may affect the placement and design of the firewall rules, but it is not a critical consideration for the IS auditor. The physical location of the firewalls refers to where they are installed or deployed in relation to the network topology, such as at the network perimeter, between network segments, or on individual hosts. The IS auditor should ensure that the firewall rules are consistent and coordinated across different locations, but this depends on the organization's security policy and network architecture.

### NEW QUESTION 193

- (Topic 2)

An organization is considering allowing users to connect personal devices to the corporate network. Which of the following should be done FIRST?

- A. Conduct security awareness training.
- B. Implement an acceptable use policy
- C. Create inventory records of personal devices
- D. Configure users on the mobile device management (MDM) solution

**Answer: B**

#### Explanation:

The first thing that should be done before allowing users to connect personal devices to the corporate network is to implement an acceptable use policy. An acceptable use policy is a document that defines the rules and guidelines for using personal devices on the corporate network, such as security requirements, access rights, responsibilities, and consequences. An acceptable use policy can help to protect the organization from potential risks such as data leakage, malware infection, or legal liability. The other options are not as important as implementing an acceptable use policy, as they do not establish the boundaries and expectations for using personal devices on the corporate network. References: CISA Review Manual, 27th Edition, page 318

### NEW QUESTION 198

.....

## **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](#)**