

# Isaca

## Exam Questions CISA

Isaca CISA



### NEW QUESTION 1

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

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

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

References:

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

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

### NEW QUESTION 2

- (Topic 3)

Which of the following should an IS auditor ensure is classified at the HIGHEST level of sensitivity?

- A. Server room access history
- B. Emergency change records
- C. IT security incidents
- D. Penetration test results

**Answer: D**

#### Explanation:

The IS auditor should ensure that penetration test results are classified at the highest level of sensitivity, because they contain detailed information about the vulnerabilities and weaknesses of the IT systems and networks, as well as the methods and tools used by the testers to exploit them. Penetration test results can be used by malicious actors to launch cyberattacks or cause damage to the organization if they are disclosed or accessed without authorization. Therefore, they should be protected with the highest level of confidentiality, integrity and availability. The other options are not as sensitive as penetration test results, because they either do not reveal as much information about the IT security posture, or they are already known or reported by the organization. References: CISA Review Manual (Digital Version)<sup>1</sup>, Chapter 5, Section 5.2.4

### NEW QUESTION 3

- (Topic 3)

Which of the following should be performed FIRST before key performance indicators (KPIs) can be implemented?

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

**Answer: B**

#### Explanation:

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

### NEW QUESTION 4

- (Topic 3)

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

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

**Answer: B**

#### Explanation:

The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been

sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 387

#### NEW QUESTION 5

- (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 6

- (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 7

- (Topic 3)

Which of the following is the BEST evidence that an organization's IT strategy is aligned to its business objectives?

- A. The IT strategy is modified in response to organizational change.
- B. The IT strategy is approved by executive management.
- C. The IT strategy is based on IT operational best practices.
- D. The IT strategy has significant impact on the business strategy

**Answer: B**

#### Explanation:

The best evidence that an organization's IT strategy is aligned to its business objectives is that the IT strategy is approved by executive management. This implies that the IT strategy has been reviewed and validated by the senior leaders of the organization, who are responsible for setting and overseeing the business objectives. The IT strategy may be modified in response to organizational change, based on IT operational best practices, or have significant impact on the business strategy, but these are not sufficient indicators of alignment without executive approval. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

#### NEW QUESTION 8

- (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 9

- (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 10

- (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)

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 15

- (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 18

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

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

? A. Improving the change management process is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While improving the change management process may help to prevent future inconsistencies or misconfigurations in application server settings, it does not ensure that the existing ones are detected and corrected.

? B. Establishing security metrics is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While establishing security metrics may help to measure and monitor the security performance and posture of application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected.

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

#### NEW QUESTION 22

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

An IS auditor reviewing the threat assessment for a data center would be most concerned if the exercise was completed by local management, because this could introduce bias, conflict of interest, or lack of expertise in the assessment process. A threat assessment is a systematic method of identifying and evaluating the potential threats that could affect the availability, integrity, or confidentiality of the data center and its assets. A threat assessment should be conducted by an independent and qualified team that has the necessary skills, knowledge, and experience to perform a comprehensive and objective analysis of the data center's

environment, vulnerabilities, and risks<sup>1</sup>.

The other options are not as concerning as option C for an IS auditor reviewing the threat assessment for a data center. Option A, some of the identified threats are unlikely to occur, is not a problem as long as the likelihood and impact of each threat are properly estimated and prioritized. A threat assessment should consider all possible scenarios, even if they have a low probability of occurrence, to ensure that the data center is prepared for any eventuality<sup>2</sup>. Option B, all identified threats relate to external entities, is not a flaw as long as the assessment also considers internal threats, such as human errors, malicious insiders, or equipment failures. External threats are often more visible and severe than internal threats, but they are not the only source of risk for a data center<sup>3</sup>. Option D, neighboring organizations' operations have been included, is not a mistake as long as the assessment also focuses on the data center's own operations. Neighboring organizations' operations may have an impact on the data center's security and availability, especially if they share physical or network infrastructure or resources. A threat assessment should take into account the interdependencies and interactions between the data center and its external environment<sup>4</sup>.

References:

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

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

? Data Center Threats and Vulnerabilities<sup>1</sup>

? Datacenter threat, vulnerability, and risk assessment<sup>2</sup>

? Data Centre Risk Assessment<sup>3</sup>

#### NEW QUESTION 26

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

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

References:

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

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

? Different Types of Inventory Fraud and How to Prevent Them<sup>1</sup>

? 6 Ways to Prevent Inventory Fraud in Your Business<sup>2</sup>

#### NEW QUESTION 29

- (Topic 3)

Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

- A. Rotating backup copies of transaction files offsite
- B. Using a database management system (DBMS) to dynamically back-out partially processed transactions
- C. Maintaining system console logs in electronic format
- D. Ensuring bisynchronous capabilities on all transmission lines

**Answer:** B

#### Explanation:

The best way to ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure is to use a database management system (DBMS) to dynamically back-out partially processed transactions. A DBMS is a software system that manages the creation, manipulation, retrieval, and security of data stored in a database. A DBMS can provide features such as transaction management, concurrency control, recovery management, and integrity management. A DBMS can dynamically back-out partially processed transactions by using mechanisms such as rollback segments, undo logs, or write-ahead logs. These mechanisms allow the DBMS to restore the database to a consistent state before the failure occurred.

References:

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

#### NEW QUESTION 32

- (Topic 3)

Which of the following is necessary for effective risk management in IT governance?

- A. Local managers are solely responsible for risk evaluation.
- B. IT risk management is separate from corporate risk management.
- C. Risk management strategy is approved by the audit committee.
- D. Risk evaluation is embedded in management processes.

**Answer:** D

#### Explanation:

The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk

management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:  
? CISA Review Manual (Digital Version)  
? CISA Questions, Answers & Explanations Database

#### NEW QUESTION 35

- (Topic 3)

An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?

- A. Analyze a new application that moots the current re
- B. Perform an analysis to determine the business risk
- C. Bring the escrow version up to date.
- D. Develop a maintenance plan to support the application using the existing code

**Answer: C**

#### Explanation:

This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version. This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements. Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application.

An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application<sup>1</sup>.

The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time-consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application<sup>2</sup>. Option B, performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk<sup>3</sup>. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code. References:

? How Important Is Source Code Escrow - ISACA<sup>1</sup>

? The What and Why of Source Code Escrow<sup>2</sup>

? Unlocking Source Code In Escrow 2023: A Guide To Secure Software<sup>3</sup>

#### NEW QUESTION 37

- (Topic 3)

An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported the auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

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

**Answer: C**

#### Explanation:

The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. An unsupported software system may have unpatched vulnerabilities that could be exploited by attackers to compromise the system or access sensitive data. By isolating the system from the rest of the network, the organization can limit the exposure and impact of a potential breach. Verifying all patches have been applied to the outdated software system, closing all unused ports on the outdated software system and monitoring network traffic attempting to reach the outdated software system are also good practices, but they do not address the root cause of the risk, which is the lack of vendor support and updates.

References:

? CISA Review Manual, 27th Edition, page 2951

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

#### NEW QUESTION 39

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

The best course of action for an IS auditor who finds that some critical recommendations have not been implemented is to evaluate senior management's acceptance of the risk. The IS auditor should understand the reasons why the recommendations have not been implemented and the implications for the organization's risk exposure. The IS auditor should also verify that senior management has formally acknowledged and accepted the residual risk and has documented the rationale and justification for their decision. The IS auditor should communicate the findings and the risk acceptance to the audit committee and other relevant stakeholders. References:



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

#### NEW QUESTION 44

- (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 45

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 46

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies. Security parameters are settings or options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies<sup>7</sup>. 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 48

- (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 way<sup>1</sup>.

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 analysis<sup>1</sup>. 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 53**

- (Topic 3)

During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed.

Which of the following is the BEST way to help management understand the associated risk?

- A. Explain the impact to disaster recovery.
- B. Explain the impact to resource requirements.
- C. Explain the impact to incident management.
- D. Explain the impact to backup scheduling.

**Answer:** A

**Explanation:**

The best way to help management understand the associated risk of missing backup cycles due to operator error and lack of exception management is to explain the impact to disaster recovery. Disaster recovery is the process of restoring normal operations and functions after a disruptive event, such as a natural disaster, a cyberattack, or a hardware failure. Backup cycles are essential for disaster recovery, because they ensure that the organization has copies of its critical data and systems that can be restored in case of data loss or corruption. If backup cycles are missed due to operator error, and these exceptions are not managed, the organization may not have the latest or complete backups available for disaster recovery, which can result in prolonged downtime, reduced productivity, lost revenue, reputational damage, and legal or regulatory penalties. The other options are not as effective as explaining the impact to disaster recovery, because they either do not address the risk of data loss or corruption, or they focus on operational or technical aspects rather than business outcomes. References: CISA Review Manual (Digital Version)<sup>1</sup>, Chapter 5, Section 5.2.1

**NEW QUESTION 57**

- (Topic 3)

Which of the following BEST facilitates the legal process in the event of an incident?

- A. Right to perform e-discovery
- B. Advice from legal counsel
- C. Preserving the chain of custody
- D. Results of a root cause analysis

**Answer:** C

**Explanation:**

The best way to facilitate the legal process in the event of an incident is to preserve the chain of custody of the evidence. The chain of custody is a record of who handled, accessed, or modified the evidence, when, where, how, and why. The chain of custody helps to ensure the integrity, authenticity, and admissibility of the evidence in a court of law. The chain of custody also helps to prevent tampering, alteration, or loss of evidence that could compromise the investigation or the prosecution. References:

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 62**

- (Topic 3)

The PRIMARY role of a control self-assessment (CSA) facilitator is to:

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

**Answer:** B

**Explanation:**

The primary role of a control self-assessment (CSA) facilitator is to focus the team on internal controls. A CSA facilitator is a person who guides the CSA process and helps the participants to identify, assess, and improve their internal controls. The facilitator does not conduct interviews, report on weaknesses, or provide solutions, as these are the responsibilities of the participants themselves<sup>1</sup>.

The other options are incorrect because they are not the primary role of a CSA facilitator. Option A, conduct interviews to gain background information, is a preliminary step that may be done by the facilitator or the participants before the CSA session, but it is not the main purpose of the facilitator. Option C, report on the internal control weaknesses, is an outcome of the CSA process that should be done by the participants who own and operate the controls. Option D, provide solutions for control weaknesses, is also an outcome of the CSA process that should be done by the participants who are in charge of implementing the improvements.

References:

? ISACA, CISA Review Manual, 27th Edition, 2019, page 2822

? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066693

? PwC, Control Self Assessments<sup>4</sup>

? Workiva, 4 factors of an effective control self-assessment (CSA) program<sup>5</sup>

**NEW QUESTION 66**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

The finding that should be the IS auditor's greatest concern is that the data model is not clearly documented. A data model is a representation of the structure, relationships, and constraints of the data used by an application. It is a vital component of the software development process, as it helps to ensure the accuracy, consistency, and quality of the data<sup>1</sup>. A clear and comprehensive documentation of the data model is essential for the maintenance and support of the application, as it facilitates the understanding, modification, and troubleshooting of the data and the application logic<sup>2</sup>.

If the organization plans to bring the support and future maintenance of the application back in-house, it will need to have access to the data model documentation from the vendor. Without it, the organization may face difficulties in transferring the knowledge and skills from the vendor to the in-house team, as well as in adapting and enhancing the application to meet changing business needs and requirements<sup>3</sup>. The lack of data model documentation may also increase the risk of errors, inconsistencies, and inefficiencies in the data and the application performance<sup>2</sup>.

The other findings are not as concerning as the lack of data model documentation, because they do not directly affect the quality and maintainability of the application. The cost of outsourcing is lower than in-house development is a benefit rather than a risk for the organization, as it implies that outsourcing has helped to save time and money for the organization<sup>4</sup>. The vendor development team is located overseas is a common practice in outsourcing, and it does not necessarily imply a lower quality or a higher risk of the application. However, it may pose some challenges in terms of communication, coordination, and cultural differences, which can be managed by establishing clear expectations, roles, and responsibilities, as well as using effective tools and methods for communication and collaboration<sup>5</sup>. A training plan for business users has not been developed is a gap that should be addressed by the organization before deploying the application, as it may affect the user acceptance and satisfaction of the application. However, it does not directly impact the quality or maintainability of the application itself. References:

? What is Data Modeling? Definition & Types | Informatica<sup>1</sup>

? Data Modeling Best Practices: Documentation | erwin<sup>2</sup>

? Data Model Documentation - an overview | ScienceDirect Topics<sup>3</sup>

? Outsourcing App Development Pros and Cons – Droids On Roids<sup>4</sup>

? 8 Risks of Software Development Outsourcing & Their Solutions - Acropolium<sup>5</sup>

? Software Training Plan: How to Create One for Your Business - Elinext

**NEW QUESTION 68**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

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

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

References:

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

? How to prevent DDoS attacks | Methods and tools | Cloudflare<sup>2</sup>

? Understanding Denial-of-Service Attacks | CISA<sup>3</sup>

#### NEW QUESTION 69

- (Topic 3)

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

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

**Answer:** C

#### Explanation:

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

References: CISA Review Manual (Digital Version)<sup>1</sup>, Chapter 5, Section 5.2.4

#### NEW QUESTION 74

- (Topic 3)

When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system. It is MOST effective for an IS auditor to review;

- A. data analytics findings.
- B. audit trails
- C. acceptance lasting results
- D. rollback plans

**Answer:** A

#### Explanation:

When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system, it is most effective for an IS auditor to review data analytics findings. Data analytics is a technique that uses software tools and statistical methods to analyze large volumes of data and identify patterns, anomalies, errors or inconsistencies. Data analytics can help to compare the source and target data sets, validate the data quality and integrity, and detect any data loss or corruption during the migration process. The other options are not as effective, because audit trails only record the actions performed on the data, acceptance testing results only verify the functionality of the new system, and rollback plans only provide contingency measures in case of migration failure.

References: CISA Review Manual (Digital Version)<sup>1</sup>, Chapter 5, Section 5.2.6

#### NEW QUESTION 77

- (Topic 3)

An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?

- A. Network penetration tests are not performed
- B. The network firewall policy has not been approved by the information security officer.
- C. Network firewall rules have not been documented.
- D. The network device inventory is incomplete.

**Answer:** A

#### Explanation:

The finding that should be ranked as the highest risk is that network penetration tests are not performed. Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices. Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If network penetration tests are not performed, the organization may not be aware of the existing or potential threats and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties. The other findings are also important, but not as risky as the lack of network penetration tests, because they either do not directly affect the network security controls, or they can be addressed by documentation or approval processes. References: CISA Review Manual (Digital Version)<sup>1</sup>, Chapter 5, Section 5.2.4

#### NEW QUESTION 78

- (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 80

- (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 230<sup>1</sup>
- ? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription<sup>2</sup>

#### NEW QUESTION 81

- (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)<sup>1</sup>, Chapter 4, Section 4.2.5

#### NEW QUESTION 85

- (Topic 3)

An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 89

- (Topic 3)

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

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



**Answer:** D

**Explanation:**

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

**NEW QUESTION 91**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies<sup>1</sup>.

The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities<sup>2</sup>. Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks<sup>2</sup>. Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other<sup>2</sup>.

References:

? Best Practice Guide: Business Continuity Planning (BCP)<sup>3</sup>

? Best Practices for Creating a Business Continuity Plan<sup>1</sup>

? Business Continuity Plan Best Practices

**NEW QUESTION 93**

- (Topic 3)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 97**

- (Topic 3)

Which of the following is MOST important when implementing a data classification program?

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

**Answer:** B

**Explanation:**

Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.

To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.

The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.

References:

? ISACA, CISA Review Manual, 27th Edition, 2020, page 247

? Data Classification: What It Is and How to Implement It

#### NEW QUESTION 101

- (Topic 3)

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

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

**Answer: D**

#### Explanation:

Segregation of duties (SoD) is a key internal control that aims to prevent fraud and errors by ensuring that no single individual can perform incompatible or conflicting tasks within a business process. SoD reduces the risk of unauthorized or improper transactions, manipulation of data, or misappropriation of assets. In the accounts payable department, SoD involves separating the following functions: invoice processing, payment authorization, payment execution, and reconciliation. For example, the person who approves an invoice should not be the same person who issues the payment or reconciles the bank statement. One of the best ways to ensure appropriate SoD within the accounts payable department is to restrict program functionality according to user security profiles. This means that each user of the accounts payable system should have a unique login and password, and should only have access to the functions that are relevant to their role and responsibilities. For instance, an invoice processor should not be able to approve payments or modify vendor records. This way, the system can enforce SoD and prevent unauthorized or fraudulent activities.

The other options are not as effective as restricting program functionality according to user security profiles. Restricting access to update programs to accounts payable staff only is a general access control measure, but it does not address the SoD issue within the accounts payable department. Including the creator's user ID as a field in every transaction record created is a useful audit trail feature, but it does not prevent users from performing incompatible functions. Ensuring that audit trails exist for transactions is a detective control that can help identify and investigate any irregularities, but it does not prevent them from occurring in the first place.

#### NEW QUESTION 104

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 106

- (Topic 2)

Which of the following is the MOST important reason to classify a disaster recovery plan (DRP) as confidential?

- A. Ensure compliance with the data classification policy.
- B. Protect the plan from unauthorized alteration.
- C. Comply with business continuity best practice.
- D. Reduce the risk of data leakage that could lead to an attack.

**Answer: D**

#### Explanation:

The most important reason to classify a disaster recovery plan (DRP) as confidential is to reduce the risk of data leakage that could lead to an attack. A DRP contains sensitive information about the organization's IT infrastructure, systems, processes, and procedures for recovering from a disaster. If this information falls into the wrong hands, it could be exploited by malicious actors to launch targeted attacks, sabotage recovery efforts, or extort ransom. Therefore, a DRP should be protected from unauthorized access, disclosure, modification, or destruction.

The other options are not as important as reducing the risk of data leakage that could lead to an attack:

? Ensuring compliance with the data classification policy is a good practice, but it is not a sufficient reason to classify a DRP as confidential. The data classification policy should reflect the level of risk and impact associated with each type of data, and a DRP should be classified as confidential based on its potential harm if compromised.

? Protecting the plan from unauthorized alteration is a valid concern, but it is not a primary reason to classify a DRP as confidential. A DRP should be protected from unauthorized alteration by implementing access controls, audit trails, version control, and change management processes. Classifying a DRP as confidential may deter some unauthorized alterations, but it does not prevent them.

? Complying with business continuity best practice is a desirable goal, but it is not a compelling reason to classify a DRP as confidential. Business continuity best practice may recommend classifying a DRP as confidential, but it does not mandate it. The decision to classify a DRP as confidential should be based on a risk assessment and a cost-benefit analysis.

#### NEW QUESTION 107

- (Topic 2)

In a RAO model, which of the following roles must be assigned to only one individual?

- A. Responsible
- B. Informed
- C. Consulted

D. Accountable

**Answer:** D

**Explanation:**

In a RAO model, which stands for Responsible, Accountable, Consulted, and Informed, the accountable role must be assigned to only one individual. The accountable role is the person who has the ultimate authority and responsibility for the outcome of the project or task, and who approves or rejects the work done by the responsible role. The accountable role cannot be delegated or shared, as it is essential to have a clear and single point of accountability for each project or task.

The other roles can be assigned to more than one individual:

? Responsible. This is the person who does the work or performs the task. There can be multiple responsible roles for different aspects or phases of a project or task, as long as they are coordinated and supervised by the accountable role.

? Informed. This is the person who needs to be notified or updated about the progress or results of the project or task. There can be multiple informed roles who have an interest or stake in the project or task, but who do not need to be consulted or involved in the decision-making process.

? Consulted. This is the person who provides input, feedback, or advice on the project or task. There can be multiple consulted roles who have expertise or experience relevant to the project or task, but who do not have the authority or responsibility to approve or reject the work done by the responsible role.

**NEW QUESTION 108**

- (Topic 2)

Due to a recent business divestiture, an organization has limited IT resources to deliver critical projects. Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

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

**Answer:** B

**Explanation:**

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

? CISA Review Manual, 27th Edition, pages 465-4661

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

**NEW QUESTION 113**

- (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 118**

- (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 123

- (Topic 2)

An organization has recently implemented a Voice-over IP (VoIP) communication system. Which of the following should be the IS auditor's PRIMARY concern?

- A. A single point of failure for both voice and data communications
- B. Inability to use virtual private networks (VPNs) for internal traffic
- C. Lack of integration of voice and data communications
- D. Voice quality degradation due to packet loss

**Answer:** A

#### Explanation:

The IS auditor's primary concern when an organization has recently implemented a Voice-over IP (VoIP) communication system is a single point of failure for both voice and data communications. VoIP is a technology that allows voice communication over IP networks such as the internet. VoIP can offer benefits such as lower costs, higher flexibility, and better integration with other applications. However, VoIP also introduces risks such as dependency on network availability, performance, and security. If both voice and data communications share the same network infrastructure and devices, then a single point of failure can affect both services simultaneously and cause significant disruption to business operations. Therefore, the IS auditor should evaluate the availability and redundancy of the network components and devices that support VoIP communication. The other options are not as critical as a single point of failure for both voice and data communications, as they do not pose a direct threat to business continuity. References: CISA Review Manual, 27th Edition, page 385

#### NEW QUESTION 124

- (Topic 2)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 126

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

Analyzing risks posed by new regulations is an appropriate role of internal audit in helping to establish an organization's privacy program. An internal auditor can provide assurance and advisory services on the compliance and effectiveness of the privacy program, as well as identify and assess the potential risks and impacts of new or changing privacy regulations. The other options are not appropriate roles of internal audit, but rather the responsibilities of the management, the information security officer, or the privacy officer. References:

? CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21

? CISA Review Questions, Answers & Explanations Database, Question ID 216

#### NEW QUESTION 130

- (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 134**

- (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 135**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

? CISA Review Manual, 27th Edition, pages 414-4151

? CISA Review Questions, Answers & Explanations Database, Question ID: 255

**NEW QUESTION 139**

- (Topic 2)

Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

- A. Ensure that the facts presented in the report are correct
- B. Communicate the recommendations to senior management
- C. Specify implementation dates for the recommendations.
- D. Request input in determining corrective action.

**Answer:** A

**Explanation:**

Ensuring that the facts presented in the report are correct is the most important thing for an IS auditor to do during an exit meeting with an auditee. An IS auditor should confirm that the audit findings and observations are accurate, complete, and supported by sufficient evidence, as well as that the auditee understands and agrees with them. This will help to avoid any misunderstandings or disputes later on, as well as to enhance the credibility and quality of the audit report. The other options are less important things for an IS auditor to do during an exit meeting, as they may involve communicating the recommendations to senior management, specifying implementation dates for the recommendations, or requesting input in determining corrective action. References:

? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21

? CISA Review Questions, Answers & Explanations Database, Question ID 222

**NEW QUESTION 140**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 143**

- (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 146**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 147**

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

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

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

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

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

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

**NEW QUESTION 152**

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 156**

- (Topic 2)

Which of the following is MOST important to consider when scheduling follow-up audits?

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

**Answer:** B

**Explanation:**

The impact if corrective actions are not taken is the most important factor to consider when scheduling follow-up audits. An IS auditor should prioritize the follow-up audits based on the risk and potential consequences of not addressing the audit findings and recommendations. The other options are less important factors that may affect the timing and scope of the follow-up audits, but not their necessity or urgency. References:

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

? CISA Review Questions, Answers & Explanations Database, Question ID 207

**NEW QUESTION 161**

- (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 162**

- (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 166

- (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 169

- (Topic 2)

Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist within the organization?

- A. Reviewing vacation patterns
- B. Reviewing user activity logs
- C. Interviewing senior IT management
- D. Mapping IT processes to roles

**Answer: D**

#### Explanation:

Mapping IT processes to roles is an activity that provides an IS auditor with the most insight regarding potential single person dependencies that might exist within the organization. Single person dependencies occur when only one person has the knowledge, skills, or access rights to perform a critical IT function. Mapping IT processes to roles can help to identify such dependencies and assess their impact on the continuity and security of IT operations. The other activities do not provide as much insight into single person dependencies, as they do not show the relationship between IT processes and roles. References: CISA Review Manual, 27th Edition, page 94

#### NEW QUESTION 173

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

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

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

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

#### NEW QUESTION 175

- (Topic 2)

Which of the following is MOST helpful for measuring benefits realization for a new system?

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

**Answer: C**

#### Explanation:

This is the most helpful method for measuring benefits realization for a new system, because it involves evaluating the actual outcomes and impacts of the system after it has been implemented and used for a certain period of time. A post-implementation review can compare the actual benefits with the expected benefits that



were defined in the business case or the benefits realization plan, and identify any gaps, issues, or opportunities for improvement. A post-implementation review can also assess the effectiveness, efficiency, and satisfaction of the system's users, stakeholders, and customers, and provide feedback and recommendations for future enhancements or changes.

The other options are not as helpful as post-implementation review for measuring benefits realization for a new system:

? Function point analysis. This is a technique that measures the size and complexity

of a software system based on the number and types of functions it provides. Function point analysis can help estimate the cost, effort, and time required to develop, maintain, or enhance a software system, but it does not measure the actual benefits or value that the system delivers to the organization or its users.

? Balanced scorecard review. This is a strategic management tool that measures the

performance of an organization or a business unit based on four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard review can help align the organization's vision, mission, and goals with its activities and outcomes, but it does not measure the specific benefits or impacts of a new system.

? Business impact analysis (BIA). This is a process that identifies and evaluates the potential effects of a disruption or disaster on the organization's critical business functions and processes. A BIA can help determine the recovery priorities, objectives, and strategies for the organization in case of an emergency, but it does not measure the benefits or value of a new system.

#### NEW QUESTION 177

- (Topic 2)

IT disaster recovery time objectives (RTOs) should be based on the:

- A. maximum tolerable loss of data.
- B. nature of the outage
- C. maximum tolerable downtime (MTD).
- D. business-defined criticality of the systems.

**Answer: D**

#### Explanation:

IT disaster recovery time objectives (RTOs) are the maximum acceptable

time that an IT system can be unavailable after a disaster before it causes unacceptable consequences for the business. IT RTOs should be based on the business-defined criticality of the systems, which reflects how important they are for supporting the business processes and functions. The maximum tolerable loss of data, the nature of the outage, and the maximum tolerable downtime (MTD) are also factors that affect the IT RTOs, but they are not the primary basis for determining them.

#### NEW QUESTION 178

- (Topic 2)

A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon. The MOST effective plan of action would be to:

- A. evaluate replacement systems and performance monitoring software.
- B. restrict functionality of system monitoring software to security-related events.
- C. re-install the system and performance monitoring software.
- D. use analytical tools to produce exception reports from the system and performance monitoring software

**Answer: D**

#### Explanation:

Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective plan of action for a company that purchased and implemented system and performance monitoring software. Exception reports are reports that highlight deviations or anomalies from predefined thresholds or standards. Using analytical tools to produce exception reports can help to reduce the size and complexity of the system and performance monitoring reports, as well as to focus on the most relevant and critical information for review and action. The other options are less effective plans of action, as they may involve unnecessary costs, risks, or efforts. References:

? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21

? CISA Review Questions, Answers & Explanations Database, Question ID 219

#### NEW QUESTION 183

- (Topic 2)

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

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

**Answer: B**

#### Explanation:

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

? CISA Review Manual (Digital Version), page 301

? CISA Questions, Answers & Explanations Database, question ID 3340

#### NEW QUESTION 186

- (Topic 2)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 187**

- (Topic 2)

Which of the following is a social engineering attack method?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 192**

- (Topic 2)

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

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

**Answer: B**

**Explanation:**

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

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

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

**NEW QUESTION 197**

- (Topic 2)

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

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

**Answer: C**

**Explanation:**

Determining accountability of data owners is the most important activity in the data classification process. Data classification is a process that assigns categories or labels to data based on their value, sensitivity, criticality and risk to the organization. Data classification helps to determine the appropriate level of protection, access and retention for data. Determining accountability of data owners is an activity that identifies and assigns roles and responsibilities for data classification,

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

#### **NEW QUESTION 200**

.....

## 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](#)**