

# Isaca

## Exam Questions CISA

Isaca CISA



#### NEW QUESTION 1

- (Topic 3)

What should an IS auditor do FIRST when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 2

- (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 3

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 4

- (Topic 3)

Which of the following 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 5

- (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 6

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

Segregation of duties (SOD) is a core internal control and an essential component of an effective risk management strategy. SOD emphasizes sharing the responsibilities of key business processes by distributing the discrete functions of these processes to multiple people and departments, helping to reduce the risk of possible errors and fraud<sup>1</sup>.

SOD is especially important in IT security, where granting excessive system access to one person or group can lead to harmful consequences, such as data breaches, identity theft, or bypassing security controls<sup>2</sup>. SOD breaks IT-related tasks into four separate function categories: authorization, custody, recordkeeping, and reconciliation<sup>1</sup>. Ideally, no one person or department holds responsibility in multiple categories.

In a role-based environment, where access privileges are granted based on predefined roles, it is important to ensure that the roles are designed and assigned in a way that supports SOD. For example, the person who develops an application should not also be the one who tests it, deploys it, or maintains it.

Therefore, an application developer should not be assigned the roles of IT operator, system administration, or database administration, as these roles may conflict with their development role and create opportunities for misuse or abuse of the system. The only role that may be assigned to an application developer without violating SOD is emergency support, which is a temporary role that allows the developer to access the system in case of a critical issue that requires immediate resolution<sup>3</sup>. However, even this role should be granted with caution and monitored closely to ensure compliance with SOD policies. References:

? ISACA, CISA Review Manual, 27th Edition, 2019, page 2824

? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066692

? Hyperproof Blog, Segregation of Duties: What it is and Why it's Important<sup>1</sup>

? Advisera Blog, Segregation of duties in your ISMS according to ISO 27001A.6.1.23

#### NEW QUESTION 7

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management.

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

? CISA Review Manual, 27th Edition, page 721

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

#### NEW QUESTION 8

- (Topic 3)

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 9

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

#### NEW QUESTION 10

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures<sup>12</sup>. Without a proper documentation of the end-to-end process, the organization may face challenges in designing, developing, testing, deploying, and monitoring the RPA solution<sup>3</sup>. References:

1: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211

2: CISA Online Review Course, Module 4: Information Systems Operations and Business

Resilience, Lesson 4.2: IT Service Delivery and Support

3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

#### NEW QUESTION 10

- (Topic 3)

An IS auditor follows up on a recent security incident and finds the incident response was not adequate. Which of the following findings should be considered MOST critical?

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

**Answer:** A

#### Explanation:

The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.

The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the



organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.

References:

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

? Incident Response Process - ISACA1

? Incident Response: How to Identify and Fix Security Weaknesses

### NEW QUESTION 12

- (Topic 3)

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

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

**Answer:** A

#### Explanation:

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

### NEW QUESTION 17

- (Topic 3)

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

- A. Review of program documentation
- B. Use of test transactions
- C. Interviews with knowledgeable users
- D. Review of source code

**Answer:** B

#### Explanation:

The most conclusive audit procedure for evaluating the effectiveness of an e-commerce application system's edit routine is to use test transactions. A test transaction is a simulated input that is processed by the system to verify its output and performance1. By using test transactions, an auditor can directly observe how the edit routine checks the validity, accuracy, and completeness of data entered by users, and how it handles incorrect or invalid data. A test transaction can also help measure the efficiency, reliability, and security of the edit routine, as well as identify any errors or weaknesses in the system. The other options are not as conclusive as using test transactions, as they rely on indirect or secondary sources of information. Reviewing program documentation is an audit procedure that involves examining the written description of the system's design, specifications, and functionality2. However, program documentation may not reflect the actual implementation or operation of the system, and it may not reveal any discrepancies or defects in the edit routine. Interviews with knowledgeable users is an audit procedure that involves asking questions to the people who use or manage the system3. However, interviews with knowledgeable users may not provide sufficient or objective evidence of the edit routine's effectiveness, and they may be influenced by personal opinions or biases. Reviewing source code is an audit procedure that involves analyzing the programming language and logic of the system4. However, reviewing source code may not be feasible or practical for complex or large systems, and it may not demonstrate how the edit routine performs in real scenarios.

### NEW QUESTION 21

- (Topic 3)

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

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

**Answer:** B

#### Explanation:

The most important thing to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization's policies and standards for data protection1. The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired2. Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is acquired3. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established

and performed after the platform is acquired<sup>4</sup>.

References:

? Cloud Messaging and Collaboration Services - Maryland.gov DoIT<sup>4</sup>

? MessageBird acquires real-time notifications and in-app messaging platform Pusher for \$35M | TechCrunch<sup>2</sup>

? Symphony to lead financial market communications with the acquisition of Cloud9 Technologies<sup>3</sup>

? Cloud messaging and collaboration | Sumo Logic

## NEW QUESTION 22

- (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 24

- (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 29

- (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 - Acropolisium<sup>5</sup>

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

### NEW QUESTION 33

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

? CISA Review Manual (Digital Version)

? CISA Questions, Answers & Explanations Database

### NEW QUESTION 38

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

Asset life cycle management is a technique of asset management where facility managers maximize the usable life of assets through planning, purchasing, using, maintaining, and disposing of assets<sup>1</sup>. The main aim of asset life cycle management is to reduce costs and increase productivity by optimizing the performance, reliability, and lifespan of assets<sup>2</sup>. Asset life cycle management can help prevent the situation of having unused applications by ensuring that the applications are aligned with the business needs, objectives, and strategies, and that they are regularly reviewed, updated, or retired as necessary<sup>3</sup>.

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

### NEW QUESTION 40

- (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 42

- (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 45

- (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 46

- (Topic 3)

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

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

**Answer: A**

#### Explanation:

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

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

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

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

? Video Surveillance Best Practices | Taylored Systems

#### NEW QUESTION 47

- (Topic 2)

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the



discrepancies were caused by problems with the organization's data quality Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

- A. Data with customer personal information
- B. Data reported to the regulatory body
- C. Data supporting financial statements
- D. Data impacting business objectives

**Answer: B**

**Explanation:**

To ensure that management concerns are addressed, internal audit should recommend that the data quality team review the data reported to the regulatory body first. This is because this data set is the most relevant and critical to the issue that triggered the enhancement of the data quality program. The data reported to the regulatory body should be accurate, complete, consistent, and timely, as any discrepancies could result in fines, penalties, or reputational damage for the organization. Data with customer personal information is important for data quality, but it is not directly related to the regulatory reporting issue. Data supporting financial statements is important for data quality, but it may not be the same as the data reported to the regulatory body. Data impacting business objectives is important for data quality, but it may not be as urgent or sensitive as the data reported to the regulatory body. References:

? CISA Review Manual, 27th Edition, pages 404-4051

? CISA Review Questions, Answers & Explanations Database, Question ID: 262

**NEW QUESTION 50**

- (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 53**

- (Topic 2)

An IS auditor is conducting a review of a data center. Which of the following observations could indicate an access control Issue?

- A. Security cameras deployed outside main entrance
- B. Antistatic mats deployed at the computer room entrance
- C. Muddy footprints directly inside the emergency exit
- D. Fencing around facility is two meters high

**Answer: C**

**Explanation:**

An IS auditor is conducting a review of a data center. An observation that could indicate an access control issue is muddy footprints directly inside the emergency exit. Access control is a process that ensures that only authorized entities or individuals can access or use an information system or resource, and prevents unauthorized access or use. Access control can be implemented using various methods or mechanisms, such as physical, logical, administrative, etc. Muddy footprints directly inside the emergency exit could indicate an access control issue, as they could suggest that someone has entered the data center through the emergency exit without proper authorization or authentication, and potentially compromised the security or integrity of the data center. Security cameras deployed outside main entrance is not an observation that could indicate an access control issue, but rather a control that could enhance access control, as security cameras are devices that capture and record video footage of the surroundings, and can help monitor and deter unauthorized access or activity. Antistatic mats deployed at the computer room entrance is not an observation that could indicate an access control issue, but rather a control that could prevent static electricity damage, as antistatic mats are devices that dissipate or reduce static charges from people or objects, and can help protect electronic equipment from electrostatic discharge (ESD). Fencing around facility is two meters high is not an observation that could indicate an access control issue, but rather a control that could improve physical security, as fencing is a barrier that encloses or surrounds an area, and can help prevent unauthorized entry or intrusion.

**NEW QUESTION 57**

- (Topic 2)

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 60**

- (Topic 2)

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

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

**Answer: B**

**Explanation:**

A nondisclosure agreement (NDA) is the best way to protect an organization's proprietary code during a joint-development activity involving a third party. An NDA is a legal contract that binds the parties involved in a joint-development activity to keep confidential any information, data or materials that are shared or exchanged during the activity. An NDA specifies what constitutes confidential information, how it can be used, disclosed or protected, how long it remains confidential, what are the exceptions and remedies for breach of confidentiality, and other terms and conditions. An NDA can help to protect an organization's proprietary code from being copied, modified, distributed or exploited by unauthorized parties without its consent or knowledge. The other options are not as effective as option B, as they do not address confidentiality issues specifically. A statement of work (SOW) is a document that defines the scope, objectives, deliverables, tasks, roles, responsibilities, timelines and costs of a joint-development activity, but it does not cover confidentiality issues explicitly. A service level agreement (SLA) is a document that defines the quality, performance and availability standards and metrics for a service provided by one party to another party in a joint-development activity, but it does not cover confidentiality issues explicitly. A privacy agreement is a document that defines how personal information collected from customers or users is collected, used, disclosed and protected by one party or both parties in a joint-development activity, but it does not cover confidentiality issues related to proprietary code. References: CISA Review Manual (Digital Version) , Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.2: Project Management Practices.

**NEW QUESTION 62**

- (Topic 2)

The PRIMARY reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?

- A. Technology risk
- B. Detection risk
- C. Control risk
- D. Inherent risk

**Answer: B**

**Explanation:**

The primary reason for an IS auditor to use data analytics techniques is to reduce detection risk. Detection risk is the risk that an IS auditor will fail to detect material errors or irregularities in the information systems environment. By using data analytics techniques, such as data extraction, analysis, visualization, and reporting, an IS auditor can enhance the audit scope, coverage, efficiency, and effectiveness. Data analytics techniques can help an IS auditor to identify anomalies, patterns, trends, correlations, and outliers in large volumes of data that may indicate potential issues or risks. Technology risk, control risk, and inherent risk are types of audit risk that are not directly affected by the use of data analytics techniques by an IS auditor. References: [ISACA Journal Article: Data Analytics for Auditors]

**NEW QUESTION 64**

- (Topic 2)

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

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

**Answer: A**

**Explanation:**

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

technology.

#### NEW QUESTION 67

- (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 68

- (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 73

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

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

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

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

#### NEW QUESTION 77

- (Topic 2)

Which of the following environments is BEST used for copying data and transformation into a compatible data warehouse format?

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

**Answer: C**

#### Explanation:

The best environment for copying data and transforming it into a compatible data warehouse format is the staging environment. The staging environment is a temporary area where data from various sources are extracted, transformed, and loaded (ETL) before being moved to the data warehouse. The staging environment allows for data cleansing, validation, integration, and standardization without affecting the source or target systems. The testing environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for verifying and validating the functionality and performance of applications or systems. The replication environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for



creating identical copies of data or systems for backup or recovery purposes. The development environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating or modifying applications or systems. References:

? CISA Review Manual, 27th Edition, pages 475-4761

? CISA Review Questions, Answers & Explanations Database, Question ID: 2642

#### NEW QUESTION 81

- (Topic 2)

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

- A. Guest operating systems are updated monthly
- B. The hypervisor is updated quarterly.
- C. A variety of guest operating systems operate on one virtual server
- D. Antivirus software has been implemented on the guest operating system only.

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 85

- (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 87

- (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 91

- (Topic 2)

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



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

**Answer:** A

**Explanation:**

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

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

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

**NEW QUESTION 95**

- (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 96**

- (Topic 2)

Stress testing should ideally be earned out under a:

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

**Answer:** A

**Explanation:**

Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:

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

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

**NEW QUESTION 98**

- (Topic 2)

Which of the following is the BEST way for an organization to mitigate the risk associated with third-party application performance?

- A. Ensure the third party allocates adequate resources to meet requirements.
- B. Use analytics within the internal audit function
- C. Conduct a capacity planning exercise
- D. Utilize performance monitoring tools to verify service level agreements (SLAs)

**Answer:** D

**Explanation:**

The best way for an organization to mitigate the risk associated with third-party application performance is to utilize performance monitoring tools to verify service level agreements (SLAs). Performance monitoring tools are software or hardware devices that measure and report the performance of an application or system, such as speed, availability, reliability, etc. Performance monitoring tools can help mitigate the risk associated with third-party application performance, by allowing the organization to verify whether the third-party provider is meeting the SLAs, which are contracts or agreements that define the expected level and quality of service for an application or system. Performance monitoring tools can also help identify and resolve any performance issues or problems that may arise from the third-party application. Ensuring the third party allocates adequate resources to meet requirements is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be feasible or effective depending on the availability, cost, and suitability of the resources. Using analytics within the internal audit function is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be timely or relevant depending on the frequency, scope, and quality of the analytics. Conducting a capacity planning exercise is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be accurate or reliable depending on the assumptions, methods, and data used for the capacity planning.

#### NEW QUESTION 99

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 101

- (Topic 2)

Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?

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

**Answer:** C

#### Explanation:

The most appropriate and effective fire suppression method for an un-staffed computer room is carbon dioxide (CO2). Carbon dioxide is a gaseous clean agent that extinguishes fire by displacing oxygen and reducing the combustion process. Carbon dioxide is suitable for un-staffed computer rooms because it does not leave any residue, damage, or corrosion on the electronic equipment, and it does not require water or other chemicals that could harm the environment or human health. However, carbon dioxide can pose a risk of asphyxiation to any person who may enter the computer room during or after the discharge, so proper safety precautions and warning signs should be in place.

The other options are not as appropriate or effective as carbon dioxide for an un-staffed computer room:

? Water sprinkler. This is a common fire suppression method that uses water to cool down and extinguish fire. However, water sprinkler is not suitable for un-staffed computer rooms because it can cause severe damage to the electronic equipment, such as short circuits, corrosion, or data loss. Water sprinkler can also create a risk of electric shock to any person who may enter the computer room during or after the discharge.

? Fire extinguishers. These are portable devices that contain a pressurized agent that can be sprayed on a fire to put it out. However, fire extinguishers are not effective for un-staffed computer rooms because they require manual operation by a trained person who can identify the type and location of the fire, and use the appropriate extinguisher. Fire extinguishers can also cause damage to the electronic equipment if they contain water or chemical agents.

? Dry pipe. This is a type of sprinkler system that uses pressurized air or nitrogen in the pipes instead of water until a fire is detected. When a fire is detected, the air or nitrogen is released and water flows into the pipes and sprinklers. However, dry pipe is not ideal for un-staffed computer rooms because it still uses water as the extinguishing agent, which can damage the electronic equipment as mentioned above. Dry pipe also has a slower response time than wet pipe sprinkler systems, which can allow the fire to spread more quickly.

#### NEW QUESTION 103

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

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

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

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

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

#### NEW QUESTION 104

- (Topic 2)

Which of the following is MOST important for an IS auditor to consider when performing the risk assessment prior to an audit engagement?

- A. The design of controls
- B. Industry standards and best practices
- C. The results of the previous audit
- D. The amount of time since the previous audit

**Answer: C**

#### Explanation:

The results of the previous audit are an important source of information for an IS auditor to consider when performing the risk assessment prior to an audit engagement, as they can provide insights into the current state and performance of the auditee, identify any issues or gaps that need to be followed up or addressed, and highlight any areas that require special attention or focus. The design of controls is an important factor to evaluate during an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not reflect the actual implementation or effectiveness of the controls. Industry standards and best practices are useful benchmarks or guidelines for an IS auditor to compare or measure against during an audit engagement, but they are not the most important thing to consider when performing the risk assessment prior to an audit engagement, as they may not be applicable or relevant to the specific context or objectives of the auditee. The amount of time since the previous audit is a relevant criterion to determine the frequency or timing of an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not indicate the level or nature of risk associated with the auditee.

#### NEW QUESTION 106

- (Topic 2)

To develop meaningful recommendations or findings, which of the following is MOST important for an IS auditor to determine and understand?

- A. Root cause
- B. Responsible party
- C. Impact
- D. Criteria

**Answer: A**

#### Explanation:

Root cause is the most important thing for an IS auditor to determine and understand to develop meaningful recommendations for findings. A root cause is the underlying factor or condition that leads to a problem or issue. A finding is a statement that describes a problem or issue identified during an audit. A recommendation is a suggestion or advice that aims to address or resolve a finding. To develop meaningful recommendations for findings, an IS auditor should determine and understand the root cause of each finding, as this can help to identify the most effective and appropriate actions to prevent or correct the problem or issue. The other options are not as important as determining and understanding the root cause, as they do not directly address or resolve the finding. References: CISA Review Manual, 27th Edition, page 434

#### NEW QUESTION 108

- (Topic 2)

Providing security certification for a new system should include which of the following prior to the system's implementation?

- A. End-user authorization to use the system in production
- B. External audit sign-off on financial controls
- C. Testing of the system within the production environment
- D. An evaluation of the configuration management practices

**Answer: D**

#### Explanation:

Providing security certification for a new system should include an evaluation of the configuration management practices prior to the system's implementation. Configuration management is a process that ensures that the system's components are identified, controlled, and tracked throughout the system's lifecycle. Configuration management helps to maintain the security and integrity of the system by preventing unauthorized or unintended changes. End-user authorization to use the system in production is not part of security certification, but rather a post-implementation activity that grants access rights to authorized users. External audit sign-off on financial controls is not part of security certification, but rather a verification activity that ensures that the system complies with financial reporting standards. Testing of the system within the production environment is not part of security certification, but rather a validation activity that ensures that the system meets the functional and performance requirements. References:

? CISA Review Manual, 27th Edition, pages 449-4501

? CISA Review Questions, Answers & Explanations Database, Question ID: 2572

#### NEW QUESTION 113

- (Topic 2)

Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

- A. Findings from prior audits
- B. Results of a risk assessment
- C. An inventory of personal devices to be connected to the corporate network
- D. Policies including BYOD acceptable user statements

**Answer: D**

#### Explanation:

The most important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program is policies including BYOD acceptable user statements. Policies are documents that define the organization's objectives, requirements, expectations, and responsibilities regarding a specific topic or area. BYOD policies should include acceptable user statements that specify what types of personal devices are allowed to connect to the corporate

network, what security measures must be implemented on those devices, what data can be accessed or stored on those devices, what actions must be taken in case of device loss or theft, and what consequences will apply for non-compliance. Policies including BYOD acceptable user statements can provide an IS auditor with a clear understanding of the scope, criteria, and objectives of the BYOD program audit. Findings from prior audits, results of a risk assessment, and an inventory of personal devices to be connected to the corporate network are also useful inputs for planning a BYOD program audit, but they are not as important as policies including BYOD acceptable user statements. References: ISACA CISA Review Manual 27th Edition, page 381.

#### NEW QUESTION 118

- (Topic 2)

Which of the following concerns is BEST addressed by securing production source libraries?

- A. Programs are not approved before production source libraries are updated.
- B. Production source and object libraries may not be synchronized.
- C. Changes are applied to the wrong version of production source libraries.
- D. Unauthorized changes can be moved into production.

**Answer: D**

#### Explanation:

Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:

? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21

? CISA Review Questions, Answers & Explanations Database, Question ID 213

#### NEW QUESTION 122

- (Topic 2)

Which of the following is the PRIMARY role of the IS auditor in an organization's information classification process?

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

**Answer: B**

#### Explanation:

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

? CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31

? CISA Review Questions, Answers & Explanations Database, Question ID 206

#### NEW QUESTION 125

- (Topic 1)

An online retailer is receiving customer complaints about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the BEST way to reduce the likelihood of future occurrences?

- A. Assign responsibility for improving data quality.
- B. Invest in additional employee training for data entry.
- C. Outsource data cleansing activities to reliable third parties.
- D. Implement business rules to validate employee data entry.

**Answer: D**

#### Explanation:

Implementing business rules to validate employee data entry is the best way to reduce the likelihood of future occurrences of poor data quality that cause customer complaints about receiving different items from what they ordered on the organization's website. Business rules are logical statements that define the conditions and actions for data validation, such as checking for data completeness, accuracy, consistency, and integrity. Assigning responsibility for improving data quality, investing in additional

employee training for data entry, and outsourcing data cleansing activities to reliable third parties are also possible ways to improve data quality, but they are not as effective as implementing business rules to validate employee data entry. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

#### NEW QUESTION 127

- (Topic 1)

Which of the following MOST effectively minimizes downtime during system conversions?

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

**Answer: D**

#### Explanation:

The most effective way to minimize downtime during system conversions is to use a parallel run. A parallel run is a method of system conversion where both the



old and new systems operate simultaneously for a period of time until the new system is verified to be functioning correctly. This reduces the risk of errors, data loss, or system failure during conversion and allows for a smooth transition from one system to another. References: CISA Review Manual, 27th Edition, page 467

#### NEW QUESTION 129

- (Topic 1)

An IS auditor is examining a front-end subledger and a main ledger. Which of the following would be the GREATEST concern if there are flaws in the mapping of accounts between the two systems?

- A. Double-posting of a single journal entry
- B. Inability to support new business transactions
- C. Unauthorized alteration of account attributes
- D. Inaccuracy of financial reporting

**Answer: D**

#### Explanation:

The greatest concern for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger is the inaccuracy of financial reporting. A subledger is a detailed record of transactions for a specific account, such as accounts receivable, accounts payable, inventory, or fixed assets. A main ledger is a summary record of all transactions for all accounts in an accounting system. The mapping of accounts between a subledger and a main ledger is the process of linking or reconciling the transactions in the subledger with the corresponding entries in the main ledger. If there are flaws in the mapping of accounts, such as missing, duplicated, or incorrect transactions, the main ledger may not reflect the true financial position and performance of the organization. This may lead to inaccurate financial reporting, which may affect decision making, compliance, auditing, taxation, and stakeholder confidence.

Double-posting of a single journal entry, inability to support new business transactions, and unauthorized alteration of account attributes are not the greatest concerns for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger. These are possible consequences or causes of flaws in the mapping of accounts, but they do not have as significant an impact as inaccuracy of financial reporting. Double-posting of a single journal entry may result in errors or discrepancies in the main ledger balances. Inability to support new business transactions may indicate limitations or inefficiencies in the accounting system design or configuration. Unauthorized alteration of account attributes may suggest weaknesses or breaches in access control or segregation of duties.

#### NEW QUESTION 132

- (Topic 1)

Which of the following is an audit reviewer's PRIMARY role with regard to evidence?

- A. Ensuring unauthorized individuals do not tamper with evidence after it has been captured
- B. Ensuring evidence is sufficient to support audit conclusions
- C. Ensuring appropriate statistical sampling methods were used
- D. Ensuring evidence is labeled to show it was obtained from an approved source

**Answer: B**

#### Explanation:

The primary role of an audit reviewer with regard to evidence is to ensure that evidence is sufficient to support audit conclusions. Evidence is the information obtained by the auditor to provide a reasonable basis for the audit opinion or findings. Evidence should be sufficient, reliable, relevant, and useful to support the audit objectives and criteria. The audit reviewer should evaluate the quality and quantity of evidence collected by the auditor and determine if it is adequate to draw valid conclusions and

recommendations. Ensuring unauthorized individuals do not tamper with evidence after it has been captured is a role of the auditor, not the audit reviewer. The auditor is responsible for safeguarding the evidence from loss, damage, or alteration during the audit process. The auditor should also document the source, date, and method of obtaining the evidence, as well as any limitations or restrictions on its use or disclosure. Ensuring appropriate statistical sampling methods were used is a role of the auditor, not the audit reviewer. The auditor is responsible for selecting an appropriate sampling method and technique that can provide sufficient evidence to achieve the audit objectives and criteria. The auditor should also document the sampling plan, population, sample size, selection method, evaluation method, and results. Ensuring evidence is labeled to show it was obtained from an approved source is a role of the auditor, not the audit reviewer. The auditor is responsible for labeling the evidence to indicate its origin, nature, and ownership. The auditor should also ensure that the evidence is obtained from reliable and credible sources that can be verified and corroborated. References: ISACA CISA Review Manual 27th Edition, page 295

#### NEW QUESTION 133

- (Topic 1)

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

- A. Walk-through reviews
- B. Substantive testing
- C. Compliance testing
- D. Design documentation reviews

**Answer: B**

#### Explanation:

Substantive testing provides the most reliable audit evidence on the validity of transactions in a financial application. Substantive testing is an audit procedure that examines the financial statements and supporting documentation to see if they contain errors or misstatements. Substantive testing can help to verify that the transactions recorded in the financial application are authorized, complete, accurate, and properly classified. Substantive testing can include methods such as vouching, confirmation, analytical procedures, or physical examination.

#### NEW QUESTION 136

- (Topic 1)

Which of the following would BEST facilitate the successful implementation of an IT-related framework?

- A. Aligning the framework to industry best practices
- B. Establishing committees to support and oversee framework activities
- C. Involving appropriate business representation within the framework
- D. Documenting IT-related policies and procedures

**Answer:** C

**NEW QUESTION 137**

- (Topic 1)

An IS auditor has found that an organization is unable to add new servers on demand in a cost-efficient manner. Which of the following is the auditor's BEST recommendation?

- A. Increase the capacity of existing systems.
- B. Upgrade hardware to newer technology.
- C. Hire temporary contract workers for the IT function.
- D. Build a virtual environment.

**Answer:** D

**Explanation:**

The best recommendation for an organization that is unable to add new servers on demand in a cost-efficient manner is to build a virtual environment. A virtual environment is a technology that allows multiple virtual machines to run on a single physical server, sharing its resources and capabilities. A virtual environment can help the organization add new servers on demand in a cost-efficient manner by reducing the need for hardware acquisition, maintenance, and power consumption. The other options are not as effective as building a virtual environment, as they do not address the root cause of the problem or provide the same benefits. Increasing the capacity of existing systems is a short-term solution that can help improve the performance and availability of the current servers, but it does not enable the organization to add new servers on demand in a cost-efficient manner. Upgrading hardware to newer technology is a costly solution that can help enhance the functionality and reliability of the servers, but it does not enable the organization to add new servers on demand in a cost-efficient manner. Hiring temporary contract workers for the IT function is an irrelevant solution that can help supplement the IT staff's skills and knowledge, but it does not enable the organization to add new servers on demand in a cost-efficient manner. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3.1

**NEW QUESTION 140**

- (Topic 1)

An IS auditor who was instrumental in designing an application is called upon to review the application. The auditor should:

- A. refuse the assignment to avoid conflict of interest.
- B. use the knowledge of the application to carry out the audit.
- C. inform audit management of the earlier involvement.
- D. modify the scope of the audit.

**Answer:** C

**Explanation:**

The IS auditor should inform audit management of the earlier involvement in designing the application. This is to ensure that there is no conflict of interest or bias that may affect the objectivity or independence of the audit. Audit management can then decide whether to assign a different auditor or to proceed with the same auditor with appropriate safeguards. The other options are not appropriate for the IS auditor to do in this situation. Refusing the assignment to avoid conflict of interest is an extreme measure that may not be necessary or feasible, especially if there are no other qualified auditors available. Using the knowledge of the application to carry out the audit is risky, as it may lead to overlooking or ignoring potential issues or errors in the application. Modifying the scope of the audit is not advisable, as it may compromise the quality or completeness of the audit. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.1

**NEW QUESTION 144**

- (Topic 1)

An IS auditor is conducting a post-implementation review of an enterprise resource planning (ERP) system. End users indicated concerns with the accuracy of critical automatic calculations made by the system. The auditor's FIRST course of action should be to:

- A. review recent changes to the system.
- B. verify completeness of user acceptance testing (UAT).
- C. verify results to determine validity of user concerns.
- D. review initial business requirements.

**Answer:** C

**Explanation:**

The IS auditor's first course of action should be to verify the results of the critical automatic calculations made by the system to determine the validity of user concerns. This is because the IS auditor needs to obtain sufficient and appropriate audit evidence to support the audit findings and conclusions. By verifying the results, the IS auditor can assess whether there are any errors or discrepancies in the system's calculations that could affect the accuracy and reliability of the financial data. The IS auditor can use various techniques to verify the results, such as re-performing the calculations, comparing them with expected values, or tracing them to source documents.

**NEW QUESTION 149**

- (Topic 1)

During the design phase of a software development project, the PRIMARY responsibility of an IS auditor is to evaluate the:

- A. Future compatibility of the application.
- B. Proposed functionality of the application.
- C. Controls incorporated into the system specifications.
- D. Development methodology employed.

**Answer:** C

**Explanation:**

The primary responsibility of an IS auditor during the design phase of a software development project is to evaluate the controls incorporated into the system specifications. Controls are mechanisms or procedures that aim to ensure the security, reliability, or performance of a system or process. System specifications are documents that define and describe the requirements, features, functions, or components of a system or software. Evaluating the controls incorporated into the

system specifications is a key responsibility of an IS auditor during the design phase of a software development project, as it helps ensure that the system or software meets the organization's objectives, standards, and expectations for security, reliability, or performance. The other options are not primary responsibilities of an IS auditor during the design phase of a software development project, as they do not directly relate to evaluating the controls incorporated into the system specifications. Future compatibility of the application is a possible factor that may affect the functionality or usability of the application in different environments or platforms, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Proposed functionality of the application is a possible factor that may affect the suitability or value of the application for meeting user needs or expectations, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Development methodology employed is a possible factor that may affect the quality or consistency of the software development process, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

**NEW QUESTION 152**

- (Topic 1)

Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

- A. Data conversion was performed using manual processes.
- B. Backups of the old system and data are not available online.
- C. Unauthorized data modifications occurred during conversion.
- D. The change management process was not formally documented

**Answer:** C

**Explanation:**

The greatest concern for an IS auditor reviewing data conversion and migration during the implementation of a new application system is unauthorized data modifications occurred during conversion. Unauthorized data modifications are changes or alterations to data that are not authorized, intended, or expected, such as due to errors, fraud, or sabotage. Unauthorized data modifications occurred during conversion can compromise the accuracy, completeness, and integrity of the data being converted and migrated to the new application system, and may result in data loss, corruption, or inconsistency. The other options are not as concerning as unauthorized data modifications occurred during conversion in reviewing data conversion and migration during the implementation of a new application system, as they do not affect the accuracy, completeness, or integrity of the data being converted and migrated. Data conversion was performed using manual processes is a possible factor that may increase the risk or complexity of data conversion and migration, but it does not necessarily imply that unauthorized data modifications occurred during conversion. Backups of the old system and data are not available online is a possible factor that may affect the availability or accessibility of the old system and data for backup or recovery purposes, but it does not imply that unauthorized data modifications occurred during conversion. The change management process was not formally documented is a possible factor that may affect the quality or consistency of the change management process for implementing the new application system, but it does not imply that unauthorized data modifications occurred during conversion. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

**NEW QUESTION 157**

- (Topic 1)

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 161**

- (Topic 1)

Which of the following is the BEST way to address segregation of duties issues in an organization with budget constraints?

- A. Rotate job duties periodically.
- B. Perform an independent audit.
- C. Hire temporary staff.
- D. Implement compensating controls.

**Answer:** D

**Explanation:**

The best way to address segregation of duties issues in an organization with budget constraints is to implement compensating controls, which are alternative controls that reduce or eliminate the risk of errors or fraud due to inadequate segregation of duties. Compensating controls may include independent reviews, reconciliations, approvals, or supervisions. Rotating job duties periodically may reduce the risk of collusion or abuse of privileges, but it may also affect operational efficiency and continuity. Performing an independent audit may detect segregation of duties issues, but it does not prevent them. Hiring temporary staff may increase operational costs and introduce new risks. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

**NEW QUESTION 162**

- (Topic 1)

Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

- A. Independent reconciliation
- B. Re-keying of wire dollar amounts

- C. Two-factor authentication control
- D. System-enforced dual control

**Answer:** D

**Explanation:**

The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System-enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and recipients by different bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system. Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

**NEW QUESTION 167**

- (Topic 1)

Which of the following is the BEST source of information for assessing the effectiveness of IT process monitoring?

- A. Real-time audit software
- B. Performance data
- C. Quality assurance (QA) reviews
- D. Participative management techniques

**Answer:** B

**Explanation:**

The best source of information for assessing the effectiveness of IT process monitoring is performance data. Performance data is a type of information that measures and reports on the results or outcomes of IT processes, such as availability, reliability, throughput, response time, or error rate. Performance data can help assess the effectiveness of IT process monitoring by providing quantitative and qualitative indicators of whether IT processes are meeting their objectives, standards, or expectations. The other options are not as good as performance data in assessing the effectiveness of IT process monitoring, as they do not provide direct or objective evidence of IT process results or outcomes. Real-time audit software is a type of tool that can help automate and facilitate audit activities, such as data collection, analysis, or reporting, but it does not provide information on IT process performance. Quality assurance (QA) reviews are a type of activity that can help evaluate and improve the quality of IT processes, products, or services, but they do not provide information on IT process performance. Participative management techniques are a type of method that can help involve and motivate IT staff in decision-making and problem-solving processes, but they do not provide information on IT process performance. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

**NEW QUESTION 172**

- (Topic 1)

Which of the following BEST guards against the risk of attack by hackers?

- A. Tunneling
- B. Encryption
- C. Message validation
- D. Firewalls

**Answer:** B

**Explanation:**

The best guard against the risk of attack by hackers is encryption. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Encryption can protect data in transit and at rest from unauthorized access, modification, or disclosure by hackers. Encryption can also ensure the authenticity and integrity of data by using digital signatures or hashes. Tunneling, message validation, and firewalls are not the best guards against the risk of attack by hackers. Tunneling is a technique that encapsulates one network protocol within another to create a secure connection between two endpoints. Message validation is a process that verifies the format, content, and origin of a message before accepting it. Firewalls are devices or software that filter network traffic based on predefined rules. These controls may help reduce the exposure or impact of hacker attacks, but they do not provide the same level of protection as encryption.

**NEW QUESTION 175**

- (Topic 1)

Which of the following is MOST important for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros?

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

**Answer:** C

**Explanation:**

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



#### NEW QUESTION 176

- (Topic 1)

An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons. Which of the following should the auditor recommend be performed FIRST?

- A. Implement a process to actively monitor postings on social networking sites.
- B. Adjust budget for network usage to include social media usage.
- C. Use data loss prevention (DLP) tools on endpoints.
- D. Implement policies addressing acceptable usage of social media during working hours.

**Answer: D**

#### Explanation:

The first course of action that the auditor should recommend after finding that several employees are spending an excessive amount of time using social media sites for personal reasons is to implement policies addressing acceptable usage of social media during working hours. Policies can help define the scope, purpose, rules, and expectations of using social media in the workplace, both for personal and professional reasons. Policies can also specify the consequences of violating the policies, such as disciplinary actions or termination. Policies can help deter employees from misusing social media at work, which could affect their productivity, performance, or security. Policies can also help protect the organization from legal liabilities or reputational damages that could arise from inappropriate or unlawful employee behavior on social media.

#### NEW QUESTION 177

- (Topic 1)

What is MOST important to verify during an external assessment of network vulnerability?

- A. Update of security information event management (SIEM) rules
- B. Regular review of the network security policy
- C. Completeness of network asset inventory
- D. Location of intrusion detection systems (IDS)

**Answer: C**

#### Explanation:

An external assessment of network vulnerability is a process of identifying and evaluating the weaknesses and risks that affect the security and availability of a network from an outsider's perspective. The most important factor to verify during this process is the completeness of network asset inventory, which is a list of all the devices, systems, and software that are connected to or part of the network. A complete and accurate network asset inventory can help identify the scope and boundaries of the network, the potential attack vectors and entry points, the critical assets and dependencies, and the existing security controls and gaps. Without a complete network asset inventory, an external assessment of network vulnerability may miss some important assets or vulnerabilities, leading to inaccurate or incomplete results and recommendations. References:

? 1 explains what is an external vulnerability scan and why it is important to have a complete network asset inventory.

? 2 provides a guide on how to conduct a full network vulnerability assessment and emphasizes the importance of knowing the network assets.

? 3 compares internal and external vulnerability scanning and highlights the need for a comprehensive network asset inventory for both types.

#### NEW QUESTION 180

- (Topic 3)

Which of the following is the BEST control to mitigate attacks that redirect Internet traffic to an unauthorized website?

- A. Utilize a network-based firewall.
- B. Conduct regular user security awareness training.
- C. Perform domain name system (DNS) server security hardening.
- D. Enforce a strong password policy meeting complexity requirement.

**Answer: C**

#### Explanation:

The best control to mitigate attacks that redirect Internet traffic to an unauthorized website is to perform domain name system (DNS) server security hardening. DNS servers are responsible for resolving domain names into IP addresses, and they are often targeted by attackers who want to manipulate or spoof DNS records to redirect users to malicious websites. By applying security best practices to DNS servers, such as encrypting DNS traffic, implementing DNSSEC, restricting access and updating patches, the organization can reduce the risk of DNS hijacking attacks. A network-based firewall, user security awareness training and a strong password policy are also important controls, but they are not as effective as DNS server security hardening in preventing this specific type of attack.

References:

? CISA Review Manual, 27th Edition, page 4021

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

#### NEW QUESTION 183

- (Topic 3)

Which of the following would be MOST effective to protect information assets in a data center from theft by a vendor?

- A. Monitor and restrict vendor activities
- B. Issue an access card to the vendor.
- C. Conceal data devices and information labels
- D. Restrict use of portable and wireless devices.

**Answer: A**

#### Explanation:

The most effective control to protect information assets in a data center from theft by a vendor is to monitor and restrict vendor activities. A vendor may have legitimate access to the data center for maintenance or support purposes, but they may also have malicious intentions or be compromised by an attacker. By monitoring and restricting vendor activities, the organization can ensure that the vendor only performs authorized tasks and does not access or tamper with sensitive data or equipment. Issuing an access card to the vendor, concealing data devices and information labels, and restricting use of portable and wireless devices are also useful controls, but they are not as effective as monitoring and restricting vendor activities in preventing theft by a vendor. References:

? CISA Review Manual, 27th Edition, page 3381

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

#### NEW QUESTION 187

- (Topic 3)

Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 189

- (Topic 3)

Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

- A. Project segments are established.
- B. The work is separated into phases.
- C. The work is separated into sprints.
- D. Project milestones are created.

**Answer:** C

#### Explanation:

The best way to enable the effectiveness of an agile project for the rapid development of a new software application is to separate the work into sprints. Sprints are short, time-boxed iterations that deliver a potentially releasable product increment at the end of each sprint. Sprints allow agile teams to work in a flexible and adaptive manner, respond quickly to changing customer needs and feedback, and deliver value faster and more frequently. Sprints also help teams to plan, execute, review, and improve their work in a collaborative and transparent way. Project segments, phases, and milestones are not specific to agile projects and do not necessarily enable the effectiveness of an agile project. References: Agile Project Management [What is it & How to Start] - Atlassian, CISA Review Manual (Digital Version).

#### NEW QUESTION 191

- (Topic 3)

Which of the following is the MOST effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented?

- A. Ensure sufficient audit resources are allocated,
- B. Communicate audit results organization-wide.
- C. Ensure ownership is assigned.
- D. Test corrective actions upon completion.

**Answer:** C

#### Explanation:

The most effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented is to ensure ownership is assigned. This means that the management of the audited area should accept responsibility for implementing the action plans and report on their progress and completion to the audit committee or senior management. This will ensure accountability, commitment, and follow-up for the audit recommendations<sup>34</sup>. References: 3: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.6: Reporting, page 41 4: CISA Online Review Course, Module 1: The Process of Auditing Information Systems, Lesson 1.6: Reporting

#### NEW QUESTION 194

- (Topic 3)

Which of the following backup schemes is the BEST option when storage media is limited?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 196

- (Topic 3)

Which of the following is a challenge in developing a service level agreement (SLA) for network services?

- A. Establishing a well-designed framework for network services.
- B. Finding performance metrics that can be measured properly
- C. Ensuring that network components are not modified by the client
- D. Reducing the number of entry points into the network

**Answer: B**

**Explanation:**

One of the challenges in developing a SLA for network services is finding performance metrics that can be measured properly and reflect the quality of service expected by the customer. Establishing a well-designed framework for network services is not a challenge, but a good practice. Ensuring that network components are not modified by the client or reducing the number of entry points into the network are security issues, not SLA issues. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 333

**NEW QUESTION 197**

- (Topic 3)

During an audit of an organization's risk management practices, an IS auditor finds several documented IT risk acceptances have not been renewed in a timely manner after the assigned expiration date. When assessing the severity of this finding, which mitigating factor would MOST significantly minimize the associated impact?

- A. There are documented compensating controls over the business processes.
- B. The risk acceptances were previously reviewed and approved by appropriate senior management
- C. The business environment has not significantly changed since the risk acceptances were approved.
- D. The risk acceptances with issues reflect a small percentage of the total population

**Answer: A**

**Explanation:**

The mitigating factor that would most significantly minimize the impact of not renewing IT risk acceptances in a timely manner is having documented compensating controls over the business processes. Compensating controls are alternative controls that reduce or eliminate the risk when the primary control is not feasible or cost-effective. The other factors, such as previous approval by senior management, unchanged business environment, and small percentage of issues, do not mitigate the risk as effectively as compensating controls. References: ISACA CISA Review Manual 27th Edition Chapter 1

**NEW QUESTION 199**

- (Topic 3)

Which of the following would MOST effectively help to reduce the number of repeated incidents in an organization?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 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](#)**