# Isaca

## Exam Questions CISA

Isaca CISA

**NEW QUESTION 1**
- (Topic 3)
Which of the following should an IS auditor ensure is classified at the HIGHEST level of sensitivity?

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

**Answer:** D

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

**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 objectives4. 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 should be of GREATEST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

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

**Answer:** D

**Explanation:**
The greatest concern for an IS auditor reviewing an organization’s business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources, procedures, communication plans, and backup arrangements3. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements. Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident4. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:
? A. The BCP’s contact information needs to be updated is not a great concern for an IS auditor reviewing an organization’s BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.
? B. The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization’s BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or effectiveness of the BCP.
? C. The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization’s BCP, as it is a high-level issue that can be resolved. Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization. Approval by senior management helps to ensure that the BCP is aligned with the organization’s strategy, objectives, and priorities, and that it has sufficient resources and authority to be implemented. Approval by senior management also helps to increase the awareness and commitment of the organization’s stakeholders to the BCP. While having no approval by senior management may affect the credibility and acceptance of the BCP, it does not affect the overall validity or effectiveness of the BCP. References: Working Toward a Managed, Mature Business Continuity Plan - ISACA, ISACA Introduces New Audit Programs for Business Continuity/Disaster …, Disaster Recovery and Business Continuity Preparedness for Cloud-based …

**NEW QUESTION 4**
- (Topic 3)
An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

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

**Answer:** B

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

**NEW QUESTION 5**
- (Topic 3)
In response to an audit finding regarding a payroll application, management implemented a new automated control. Which of the following would be MOST helpful to the IS auditor when evaluating the effectiveness of the new control?

A. Approved test scripts and results prior to implementation
B. Written procedures defining processes and controls
C. Approved project scope document
D. A review of tabletop exercise results

**Answer:** B

**Explanation:**
The best way to evaluate the effectiveness of a new automated control is to review the written procedures that define the processes and controls. This will help the IS auditor to understand the objectives, scope, roles, responsibilities, and expected outcomes of the control. The written procedures will also provide a basis for testing the control and verifying its compliance with the audit finding recommendations. References:
? ISACA Frameworks: Blueprints for Success
? CISA Review Manual (Digital Version)

**NEW QUESTION 6**
- (Topic 3)
Which of the following is necessary for effective risk management in IT governance?

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

**Answer:** D

**Explanation:**
The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:
? CISA Review Manual (Digital Version)
? CISA Questions, Answers & Explanations Database

**NEW QUESTION 7**
- (Topic 3)
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?

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

**Answer:** C

**Explanation:**
This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version. This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements.
Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application.
An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application1.
The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time-consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application2. Option B,

performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk3. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code. References:
? How Important Is Source Code Escrow - ISACA1
? The What and Why of Source Code Escrow2
? Unlocking Source Code In Escrow 2023: A Guide To Secure Software3

**NEW QUESTION 8**
- (Topic 3)
Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

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

**Answer:** C

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

**NEW QUESTION 9**
- (Topic 3)
Which of the following BEST describes an audit risk?

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

**Answer:** B

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

**NEW QUESTION 10**
- (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 acquired4.
References:
? Cloud Messaging and Collaboration Services - Maryland.gov DoIT4

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

**NEW QUESTION 10**
- (Topic 3)
During an exit meeting, an IS auditor highlights that backup cycles are being missed due to operator error and that these exceptions are not being managed. Which of the following is the BEST way to help management understand the associated risk?

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

**Answer:** A

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

**NEW QUESTION 12**
- (Topic 3)
Which of the following provides the BEST providence that outsourced provider services are being properly managed?

A. The service level agreement (SLA) includes penalties for non-performance.
B. Adequate action is taken for noncompliance with the service level agreement (SLA).
C. The vendor provides historical data to demonstrate its performance.
D. Internal performance standards align with corporate strategy.

**Answer:** B

**Explanation:**
Adequate action taken for noncompliance with the service level agreement (SLA) provides the best evidence that outsourced provider services are being properly managed. This shows that the organization is monitoring the performance of the provider and enforcing the terms of the SLA.
The other options are not as convincing as evidence of proper management. Option A, the SLA includes penalties for non-performance, is a good practice but does not guarantee that the penalties are actually applied or that the performance is satisfactory. Option C, the vendor provides historical data to demonstrate its performance, is not reliable because the data may be biased or inaccurate. Option D, internal performance standards align with corporate strategy, is irrelevant to the question of outsourced provider management. References:
? ISACA, CISA Review Manual, 27th Edition, 2019, page 2821
? ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066692

**NEW QUESTION 15**
- (Topic 3)
An IS auditor assessing the controls within a newly implemented call center would First

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

**Answer:** D

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

**NEW QUESTION 20**
- (Topic 3)
Which of the following is the BEST way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC)?

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

**Answer:** B

**Explanation:**
The best way to mitigate the risk associated with unintentional modifications of complex calculations in end-user computing (EUC) is to execute copies of EUC programs out of a secure library. This will ensure that the original EUC programs are protected from unauthorized changes and that the copies are run in a controlled environment. A secure library is a repository of EUC programs that have been tested, validated, and approved by the appropriate authority. Executing

copies of EUC programs out of a secure library can also help with version control, backup, and recovery of EUC programs. Having an independent party review the source calculations, implementing complex password controls, and verifying EUC results through manual calculations are not as effective as executing copies of EUC programs out of a secure library, as they do not prevent or detect unintentional modifications of complex calculations in EUC. References:
End-User Computing (EUC) Risks: A Comprehensive Guide, End User Computing (EUC) Risk Management

**NEW QUESTION 22**
- (Topic 3)
Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

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

**Answer:** B

**Explanation:**
The best way to detect that a distributed denial of service (DDoS) attack is occurring is to use automated monitoring of logs. A DDoS attack disrupts the operations of a server, service, or network by flooding it with unwanted Internet traffic2. Automated monitoring of logs can help pinpoint potential DDoS attacks by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and alerting administrators or security teams of any anomalies or malicious requests, protocols, or IP blocks3. Automated monitoring of logs can also help identify the source, type, and impact of the DDoS attack, and provide evidence for further investigation or mitigation.
The other options are not as effective as automated monitoring of logs for detecting DDoS attacks. Customer service complaints are an indirect and delayed indicator of a DDoS attack, as they rely on users reporting problems with accessing a website or service. Customer service complaints may also be caused by other factors unrelated to DDoS attacks, such as server errors or network issues. Server crashes are an extreme and undesirable indicator of a DDoS attack, as they indicate that the server has already been overwhelmed by the attack and has stopped functioning. Server crashes may also result in data loss or corruption, service disruption, or reputational damage. Penetration testing is a proactive and preventive measure for assessing the security posture of a system or network, but it does not detect ongoing DDoS attacks. Penetration testing may involve simulating DDoS attacks to test the resilience or vulnerability of a system or network, but it does not monitor real-time traffic or identify actual attackers.
References:
? ISACA CISA Review Manual 27th Edition (2019), page 254
? How to prevent DDoS attacks | Methods and tools | Cloudflare2
? Understanding Denial-of-Service Attacks | CISA3

**NEW QUESTION 26**
- (Topic 3)
Which of the following would be of GREATEST concern when reviewing an organization's security information and event management (SIEM) solution?

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

**Answer:** C

**Explanation:**
The greatest concern that the IS auditor should have when reviewing an organization’s security information and event management (SIEM) solution is that the SIEM is decentralized. This is because a decentralized SIEM can pose challenges for collecting, correlating, analyzing and reporting on security events and incidents from multiple sources and locations. A decentralized SIEM can also increase the complexity and cost of maintaining and updating the SIEM components, as well as the risk of inconsistent or incomplete security monitoring and response. The IS auditor should recommend that the organization adopts a centralized or hybrid SIEM architecture that can provide a holistic and integrated view of the security posture and activities across the organization. The other findings are not as concerning as a decentralized SIEM, because they can be addressed by implementing best practices and standards for SIEM reporting and configuration.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

**NEW QUESTION 27**
- (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 32**
- (Topic 3)
An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?

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

**Answer:** A

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

**NEW QUESTION 37**
- (Topic 3)
Which of the following is the BEST metric to measure the alignment of IT and business strategy?

A. Level of stakeholder satisfaction with the scope of planned IT projects
B. Percentage of enterprise risk assessments that include IT-related risk
C. Percentage of stat satisfied with their IT-related roles
D. Frequency of business process capability maturity assessments

**Answer:** B

**Explanation:**
The best metric to measure the alignment of IT and business strategy is the percentage of enterprise risk assessments that include IT-related risk. This metric indicates how well the organization identifies and manages the IT risks that could affect its strategic objectives and performance. A high percentage of enterprise risk assessments that include IT-related risk shows that the organization considers IT as an integral part of its business strategy and aligns its IT resources and capabilities with its business needs and goals. References: : CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.2: IT Strategy, page 67 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.2: IT Strategy

**NEW QUESTION 40**
- (Topic 3)
Which of the following would be MOST useful when analyzing computer performance?

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

**Answer:** A

**Explanation:**
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
References:
? What is Computer Performance?
? How to Measure Computer Performance

**NEW QUESTION 45**
- (Topic 3)
Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

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

**Answer:** B

**Explanation:**
The most important consideration for an IS auditor when assessing the adequacy of an organization’s information security policy is the business objectives. An information security policy is a document that defines the organization’s approach to protecting its information assets from internal and external threats. It should align with the organization’s mission, vision, values, and goals, and support its business processes and functions1. An information security policy should also be focused on the business needs and requirements of the organization, rather than on technical details or specific solutions2. The other options are not as important as the business objectives, because they do not directly reflect the organization’s purpose and direction. IT steering committee minutes are records of the discussions and decisions made by a group of senior executives who oversee the IT strategy and governance of the organization. They may provide some insights into the information security policy, but they are not sufficient to evaluate its adequacy3. Alignment with the IT tactical plan is a measure of how well the information security policy supports the short-term actions and projects that implement the IT strategy. However, the IT tactical plan itself should be aligned with the business

objectives, and not vice versa4. Compliance with industry best practice is a desirable quality of an information security policy, but it is not a guarantee of its effectiveness or suitability for the organization. Industry best practices are general guidelines or recommendations that may not apply to every organization or situation. An information security policy should be customized and tailored to the specific context and needs of the organization. References:
? The 12 Elements of an Information Security Policy | Exabeam1
? 11 Key Elements of an Information Security Policy | Egnyte2
? What is an IT steering committee? Definition, roles & responsibilities …3
? What is IT Strategy? Definition, Components & Best Practices | BMC …4
? IT Security Policy: Key Components & Best Practices for Every Business

**NEW QUESTION 47**
- (Topic 3)
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

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

**Answer:** C

**Explanation:**
The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential information from the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy. References:
? CISA Review Manual, 27th Edition, page 2301
? CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

**NEW QUESTION 51**
- (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 55**
- (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 58**
- (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 61**
- (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 center1
? Data Center Security: Checklist and Best Practices | Kisi2
? Video Surveillance Best Practices | Taylored Systems

**NEW QUESTION 64**
- (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 67**
- (Topic 2)
Which of the following documents should specify roles and responsibilities within an IT audit organization?

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

**Answer:** B

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

**NEW QUESTION 68**
- (Topic 2)
An organization has recently implemented a Voice-over IP (VoIP) communication system. Which ot the following should be the IS auditor's PRIMARY concern?

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

**Answer:** A

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

**NEW QUESTION 69**
- (Topic 2)
Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

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

**Answer:** A

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

**NEW QUESTION 70**
- (Topic 2)
Which of the following is the BEST indicator of the effectiveness of an organization's incident response program?

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

**Answer:** C

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

**NEW QUESTION 71**
- (Topic 2)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

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

**Answer:** C

**Explanation:**
The most important factor for the organization to ensure when reducing the retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for defining the retention and disposal requirements for the data under their custody, based on business, legal, regulatory, and contractual obligations. The policy should reflect the data owner's decisions and obtain their approval. The policy should also include a risk-based approach, but this is not as important as complying with data owner responsibilities. The retention period should allow for review during the year-end audit, but this may not be necessary for low-value transactions that have minimal impact on financial reporting. The total transaction amount may have some impact on financial reporting, but this is not a direct consequence of reducing the retention period. References:
? CISA Review Manual, 27th Edition, pages 414-4151
? CISA Review Questions, Answers & Explanations Database, Question ID: 255

**NEW QUESTION 74**
- (Topic 2)
Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

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

**Answer:** A

**Explanation:**
Ensuring that the facts presented in the report are correct is the most important thing for an IS auditor to do during an exit meeting with an auditee. An IS auditor should confirm that the audit findings and observations are accurate, complete, and supported by sufficient evidence, as well as that the auditee understands and agrees with them. This will help to avoid any misunderstandings or disputes later on, as well as to enhance the credibility and quality of the audit report. The other options are less important things for an IS auditor to do during an exit meeting, as they may involve communicating the recommendations to senior management, specifying implementation dates for the recommendations, or requesting input in determining corrective action. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21
? CISA Review Questions, Answers & Explanations Database, Question ID 222

**NEW QUESTION 78**
- (Topic 2)
The IS quality assurance (OA) group is responsible for:

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

**Answer:** A

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

**NEW QUESTION 80**
- (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 lo 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 82**
- (Topic 2)
Which of the following is MOST important to consider when scheduling follow-up audits?

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

**Answer:** B

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

**NEW QUESTION 86**
- (Topic 2)
Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm tor 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 89**
- (Topic 2)
Which of the following findings from an IT governance review should be of GREATEST concern?

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

**Answer:** C

**Explanation:**
IT value analysis has not been completed is a finding from an IT governance review that should be of greatest concern. IT value analysis is a process of measuring and demonstrating the contribution of IT to the organization’s goals and objectives. An IS auditor should be concerned about the lack of IT value analysis, as it may indicate that the IT investments and resources are not aligned with the business needs and expectations, or that the IT performance and outcomes are not monitored and evaluated. The other options are less critical findings that may not have a significant impact on the IT governance. References:
? CISA Review Manual (Digital Version), Chapter 5, Section 5.11
? CISA Review Questions, Answers & Explanations Database, Question ID 218

**NEW QUESTION 93**
- (Topic 2)
A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon The MOST effective plan of action would be to:

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

**Answer:** D

**Explanation:**
Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective plan of action for a company that purchased and implemented system and performance monitoring software. Exception reports are reports that highlight deviations or anomalies from predefined thresholds or standards. Using analytical tools to produce exception reports can help to reduce the size and complexity of the system and performance monitoring reports, as well as to focus on the most relevant and critical information for review and action. The other options are less effective plans of action, as they may involve unnecessary costs, risks, or efforts. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
? CISA Review Questions, Answers & Explanations Database, Question ID 219

**NEW QUESTION 95**
- (Topic 2)
Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS audit has been asked to conduct a control assessment. the auditor's BEST course of action would be to determine if:

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

**Answer:** B

**Explanation:**
The auditor's best course of action after a security breach in which a hacker exploited a well-known vulnerability in the domain controller is to determine if the logs were monitored. Log monitoring is an essential control for detecting and responding to security incidents, especially when known vulnerabilities exist in the system. The auditor should assess if the logs were properly configured, collected, reviewed, analyzed, and acted upon by the responsible parties. Updating patches, monitoring network traffic, and classifying domain controllers for high availability are also important controls, but they are not directly related to the detection and response of the security breach. References:
? CISA Review Manual (Digital Version), page 301
? CISA Questions, Answers & Explanations Database, question ID 3340

**NEW QUESTION 96**
- (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 101**
- (Topic 2)
When testing the adequacy of tape backup procedures, which step BEST verifies that regularly scheduled Backups are timely and run to completion?

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

**Answer:** D

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

**NEW QUESTION 103**
- (Topic 2)
Which of the following occurs during the issues management process for a system development project?

A. Contingency planning
B. Configuration management
C. Help desk management
D. Impact assessment

**Answer:** D

**Explanation:**
Impact assessment is an activity that occurs during the issues management process for a system development project. Issues management is a process of identifying, analyzing, resolving, and monitoring issues that may affect the project scope, schedule, budget, or quality. Impact assessment is a technique of evaluating the severity and priority of an issue, as well as its implications for the project objectives and deliverables. The other options are not activities that occur during the issues management process, but rather related to other processes such as contingency planning, configuration management, or help desk management. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
? CISA Review Questions, Answers & Explanations Database, Question ID 217

**NEW QUESTION 105**
- (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 109**
- (Topic 2)
The BEST way to determine whether programmers have permission to alter data in the production environment is by reviewing:

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

**Answer:** D

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

**NEW QUESTION 114**
- (Topic 2)
An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

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

**Answer:** C

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

**NEW QUESTION 115**
- (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 120**
- (Topic 2)
An organization has developed mature risk management practices that are followed across all departments What is the MOST effective way for the audit team to leverage this risk management maturity?

A. Implementing risk responses on management's behalf
B. Integrating the risk register for audit planning purposes
C. Providing assurances to management regarding risk
D. Facilitating audit risk identification and evaluation workshops

**Answer:** B

**Explanation:**
The most effective way for the audit team to leverage the risk management maturity of the organization is to integrate the risk register for audit planning purposes. The risk register is a document that records the identified risks, their likelihood, impact, and mitigation strategies for a project or an organization. By using the risk register, the audit team can align their audit objectives, scope, and procedures with the organization’s risk profile and priorities. This will help the audit team to provide more value-added and relevant assurance and recommendations to the management and stakeholders.
Some of the web sources that support this answer are:
? Audit Maturity And Risk Management | Ideagen
? Building a Mature Enterprise Risk Management Plan | AuditBoard
? CISA Certified Information Systems Auditor – Question0551

**NEW QUESTION 125**
- (Topic 2)
Which of the following is the PRIMARY reason to follow a configuration management process to maintain application?

A. To optimize system resources
B. To follow system hardening standards
C. To optimize asset management workflows
D. To ensure proper change control

**Answer:** D

**Explanation:**
Following a configuration management process to maintain applications is the primary reason for ensuring proper change control. Configuration management is a process of identifying, documenting, controlling, and verifying the configuration items and their interrelationships within an IT system or environment. Following a configuration management process can help to ensure that any changes to the applications are authorized, tested, documented, and tracked throughout their lifecycle. This will help to prevent unauthorized or improper changes that could affect the functionality, performance, or security of the applications. The other options are not the primary reasons for following a configuration management process, but rather possible benefits or outcomes of doing so. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
? CISA Review Questions, Answers & Explanations Database, Question ID 225

**NEW QUESTION 128**
- (Topic 2)
An IS auditor notes that IT and the business have different opinions on the availability of their application servers. Which of the following should the IS auditor review FIRST in order to understand the problem?

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

**Answer:** A

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

**NEW QUESTION 129**
- (Topic 2)
The due date of an audit project is approaching, and the audit manager has determined that only 60% of the audit has been completed. Which of the following should the audit manager do FIRST?

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

**Answer:** A

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

**NEW QUESTION 134**
- (Topic 2)
An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

A. The security of the desktop PC is enhanced.
B. Administrative security can be provided for the client.
C. Desktop application software will never have to be upgraded.
D. System administration can be better managed

**Answer:** C

**Explanation:**
The major advantage of moving from many desktop PCs to a thin client architecture is that desktop application software will never have to be upgraded. A thin client architecture is a type of client-server architecture that uses lightweight or minimal devices (thin clients) as clients that connect to a central server that provides most of the processing and storage functions. A thin client architecture can offer several benefits over a traditional desktop PC architecture, such as lower cost, higher security, easier maintenance, etc. One of these benefits is that desktop application software will never have to be upgraded on thin clients, as all the applications are installed and updated on the server, and accessed by thin clients through a network connection. This can save time and money for installing and upgrading software on individual devices, and ensure consistency and compatibility among different devices. The security of the desktop PC is enhanced is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can enhance the security of desktop PCs by reducing the exposure or vulnerability of data and applications on individual devices, and centralizing the security management and control on the server. However, this advantage may depend on other factors such as network security, server security, user authentication, etc. Administrative security can be provided for the client is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can provide administrative security for clients by allowing administrators to configure and manage client devices remotely from the server, and enforce policies and restrictions on client access or usage. However, this advantage may depend on other factors such as network reliability, server availability, user compliance, etc. System administration can be better managed is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can improve system administration by simplifying and streamlining the tasks and activities involved in maintaining and supporting client devices, such as backup, recovery, troubleshooting, etc., and consolidating them on the server. However, this advantage may depend on other factors such as network bandwidth, server capacity, user satisfaction

**NEW QUESTION 135**
- (Topic 2)
In an online application, which of the following would provide the MOST information about the transaction audit trail?

A. System/process flowchart
B. File layouts
C. Data architecture
D. Source code documentation

**Answer:** C

**Explanation:**
In an online application, data architecture provides the most information about the transaction audit trail, as it describes how data are created, stored, processed, accessed and exchanged among different components of the application. Data architecture includes data models, schemas, dictionaries, metadata, standards and policies that define the structure, quality, integrity, security and governance of data. Data architecture can help the IS auditor to trace the origin, flow, transformation and destination of data in an online transaction, and to identify the key data elements, attributes and relationships that are relevant for audit purposes. A system/process flowchart is a graphical representation of the sequence of steps or activities that are performed by a system or process. A system/process flowchart can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. A system/process flowchart shows the inputs, outputs, decisions and actions of a system or process, but it does not show the data elements, attributes and relationships that are involved in each step or activity. A file layout is a specification of the format and structure of a data file. A file layout can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. A file layout shows the fields, types, lengths and positions of data in a file, but it does not show the origin, flow, transformation and destination of data in an online transaction. Source code documentation is a description of the logic, functionality and purpose of a program or module written in a programming language. Source code documentation can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. Source code documentation shows the instructions, variables and parameters that are used to perform calculations and operations on data, but it does not show the data elements, attributes and relationships that are involved in each instruction or operation. References: CISA Review Manual (Digital Version) 1, Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: Data Administration Practices.

**NEW QUESTION 137**
- (Topic 2)
Which of the following would BEST manage the risk of changes in requirements after the analysis phase of a business application development project?

A. Expected deliverables meeting project deadlines
B. Sign-off from the IT team
C. Ongoing participation by relevant stakeholders
D. Quality assurance (OA) review

**Answer:** B

**NEW QUESTION 138**
- (Topic 2)
During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related
to managing data risk. What should the auditor do FIRST?

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

**Answer:** A

**Explanation:**
Asking management why the regulatory changes have not been included is the first thing that an IS auditor should do during the planning stage of a compliance audit. An IS auditor should inquire about the reasons for not updating the inventory of compliance requirements with recent regulatory changes related to managing data risk. This will help the IS auditor to understand whether there is a gap in awareness, communication, or implementation of compliance obligations within the organization. The other options are not the first things that an IS auditor should do, but rather possible subsequent actions that may depend on management's response. References:
? CISA Review Manual (Digital Version), Chapter 2, Section 2.31
? CISA Review Questions, Answers & Explanations Database, Question ID 214

**NEW QUESTION 141**
- (Topic 2)
An IS auditor should ensure that an application's audit trail:

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

**Answer:** A

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

**NEW QUESTION 143**
- (Topic 2)
The GREATEST benefit of using a polo typing approach in software development is that it helps to:

A. minimize scope changes to the system.
B. decrease the time allocated for user testing and review.
C. conceptualize and clarify requirements.
D. Improve efficiency of quality assurance (QA) testing

**Answer:** C

**Explanation:**
The greatest benefit of using a prototyping approach in software development is that it helps to conceptualize and clarify requirements. A prototyping approach is a method of creating a simplified or partial version of a software product to demonstrate its features and functionality. A prototyping approach can help to elicit, validate, and refine the requirements of the software product, as well as to obtain feedback from the users and stakeholders. The other options are not the greatest benefits of using a prototyping approach, but rather possible outcomes or advantages of doing so. References:
? CISA Review Manual (Digital Version), Chapter 4, Section 4.3.11
? CISA Review Questions, Answers & Explanations Database, Question ID 227

**NEW QUESTION 146**
- (Topic 2)

Capacity management enables organizations to:

A. forecast technology trends
B. establish the capacity of network communication links
C. identify the extent to which components need to be upgraded
D. determine business transaction volumes.

**Answer:** C

**Explanation:**
Capacity management is a process that ensures that the IT resources of an organization are sufficient to meet the current and future demands of the business. Capacity management enables organizations to identify the extent to which components need to be upgraded, by monitoring and analyzing the performance, utilization, and availability of the IT components, such as servers, networks, storage, applications, etc., and identifying any bottlenecks, gaps, or risks that may affect the service level agreements (SLAs) or quality of service (QoS). Capacity management also helps organizations to plan and optimize the use of IT resources, by forecasting the future demand and growth of the business, and aligning the IT capacity with the business needs and objectives. Forecasting technology trends is a possible outcome of capacity management, but it is not its main purpose. Establishing the capacity of network communication links is a part of capacity management, but it is not its main goal. Determining business transaction volumes is an input for capacity management, but it is not its main objective.

**NEW QUESTION 151**
- (Topic 2)
An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

A. violation reports may not be reviewed in a timely manner.
B. a significant number of false positive violations may be reported.
C. violations may not be categorized according to the organization's risk profile.
D. violation reports may not be retained according to the organization's risk profile.

**Answer:** C

**NEW QUESTION 153**
- (Topic 2)
After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

A. Verifying that access privileges have been reviewed
B. investigating access rights for expiration dates
C. Updating the continuity plan for critical resources
D. Updating the security policy

**Answer:** A

**Explanation:**
The most important task for an IS auditor to perform after the merger of two organizations is to verify that access privileges have been reviewed. Access privileges are the permissions granted to users, groups, or roles to access, modify, or manage IT resources, such as systems, applications, data, or networks. After a merger, the IS auditor should ensure that the access privileges of both organizations are aligned with the new business objectives, policies, and processes, and that there are no conflicts, overlaps, or gaps in the access rights. The IS auditor should also verify that the access privileges are based on the principle of least privilege, which means that users are granted only the minimum level of access required to perform their tasks.
The other options are not as important as verifying that access privileges have been reviewed:
? Investigating access rights for expiration dates is a useful task, but it is not the most important one. Expiration dates are the dates when access rights are automatically revoked or suspended after a certain period of time or after a specific event. The IS auditor should check that the expiration dates are set appropriately and enforced consistently, but this is not as critical as reviewing the access privileges themselves.
? Updating the continuity plan for critical resources is a necessary task, but it is not the most urgent one. A continuity plan is a document that outlines the procedures and actions to be taken in the event of a disruption or disaster that affects the availability of IT resources. The IS auditor should update the continuity plan to reflect the changes and dependencies introduced by the merger, but this can be done after verifying that the access privileges are secure and compliant.
? Updating the security policy is an essential task, but it is not the most immediate one. A security policy is a document that defines the rules and guidelines for securing IT resources and protecting information assets. The IS auditor should update the security policy to incorporate the best practices and standards of both organizations, and to address any new risks or threats posed by the merger, but this can be done after verifying that the access privileges are aligned with the policy.

**NEW QUESTION 158**
- (Topic 2)
During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements Which of the following is the BEST way to obtain this assurance?

A. Review sign-off documentation
B. Review the source code related to the calculation
C. Re-perform the calculation with audit software
D. Inspect user acceptance lest (UAT) results

**Answer:** C

**Explanation:**
The best way to obtain assurance that certain automated calculations comply with the regulatory requirements is to re-perform the calculation with audit software. This will allow the auditor to independently verify the accuracy and validity of the calculation and compare it with the expected results. Reviewing sign-off documentation, source code, or user acceptance test results may not provide sufficient evidence or assurance that the calculation is correct and compliant.
References:
? CISA Review Manual (Digital Version), page 325
? CISA Questions, Answers & Explanations Database, question ID 3335

**NEW QUESTION 162**
- (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 165**
- (Topic 2)
Which of the following MUST be completed as part of the annual audit planning process?

A. Business impact analysis (BIA)
B. Fieldwork
C. Risk assessment
D. Risk control matrix

**Answer:** C

**Explanation:**
Risk assessment is a mandatory part of the annual audit planning process, as it helps to identify and prioritize the areas that pose the highest risk to the organization's objectives and operations. Risk assessment involves analyzing the internal and external factors that affect the organization's risk profile, evaluating the likelihood and impact of potential events or scenarios, assessing the existing controls and mitigation strategies, and determining the residual risk level. Based on the risk assessment results, the IS auditor can allocate resources and schedule audits accordingly. A business impact analysis (BIA) is a process that identifies and evaluates the critical business functions and processes that could be disrupted by a disaster or incident, and estimates the potential impact on the organization's operations, reputation and finances. A BIA is not a mandatory part of the annual audit planning process, but it can be used as an input for risk assessment or as a subject for audit. Fieldwork is the phase of an audit where the IS auditor collects evidence to support the audit objectives and conclusions. Fieldwork is not part of the annual audit planning process, but it is part of each individual audit engagement. A risk control matrix is a tool that maps the risks identified in a risk assessment to the controls that mitigate them. A risk control matrix is not a mandatory part of the annual audit planning process, but it can be used as an output of risk assessment or as a tool for audit testing. References:
CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.2: Audit Planning.

**NEW QUESTION 170**
- (Topic 2)
Which of the following are BEST suited for continuous auditing?

A. Low-value transactions
B. Real-lime transactions
C. Irregular transactions
D. Manual transactions

**Answer:** B

**Explanation:**
Continuous auditing is a method of performing audit-related activities on a real-time or near real-time basis. Continuous auditing is best suited for real-time transactions, such as online banking, e-commerce, or electronic funds transfer, that require immediate verification and assurance. Low-value transactions are not necessarily suitable for continuous auditing, as they may not pose significant risks or require frequent monitoring. Irregular transactions are not suitable for continuous auditing, as they may not occur frequently or consistently enough to justify the use of continuous auditing techniques. Manual transactions are not suitable for continuous auditing, as they may not be captured or processed by automated systems that enable continuous auditing. References:
? CISA Review Manual, 27th Edition, pages 307-3081
? CISA Review Questions, Answers & Explanations Database, Question ID: 253

**NEW QUESTION 175**
- (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 178**
- (Topic 2)
Which of the following is the BEST source of information tor an IS auditor to use when determining whether an organization's information security policy is adequate?

A. Information security program plans
B. Penetration test results
C. Risk assessment results
D. Industry benchmarks

**Answer:** C

**Explanation:**
The best source of information for an IS auditor to use when determining whether an organization's information security policy is adequate is the risk assessment results. The risk assessment results provide the auditor with an overview of the organization's risk profile, including the identification, analysis, and evaluation of the risks that affect the confidentiality, integrity, and availability of the information assets. The auditor can use the risk assessment results to compare the organization's information security policy with the risk appetite, risk tolerance, and risk treatment strategies of the organization. The auditor can also use the risk assessment results to evaluate if the information security policy is aligned with the organization's objectives, requirements, and regulations.
Some of the web sources that support this answer are:
? Performance Measurement Guide for Information Security
? ISO 27001 Annex A.5 - Information Security Policies
? [CISA Certified Information Systems Auditor – Question0551]

**NEW QUESTION 179**
- (Topic 2)
Which of the following should an IS auditor consider the MOST significant risk associated with a new health records system that replaces a legacy system?

A. Staff were not involved in the procurement process, creating user resistance to the new system.
B. Data is not converted correctly, resulting in inaccurate patient records.
C. The deployment project experienced significant overruns, exceeding budget projections.
D. The new system has capacity issues, leading to slow response times for users.

**Answer:** B

**Explanation:**
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as
significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition], page 281.

**NEW QUESTION 181**
- (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 185**
- (Topic 1)
Due to limited storage capacity, an organization has decided to reduce the actual retention period for media containing completed low-value transactions. Which of the following is MOST important for the organization to ensure?

A. The policy includes a strong risk-based approach.

B. The retention period allows for review during the year-end audit.
C. The total transaction amount has no impact on financial reporting.
D. The retention period complies with data owner responsibilities.

**Answer:** D

**Explanation:**
The most important thing for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for the quality, security, and availability of the data under their control. They are also responsible for defining and enforcing data retention policies that comply with legal, regulatory, contractual, and business requirements. Data owners should be consulted and involved in any decision that affects the retention period of their data, as they are ultimately liable for any consequences of data loss or breach.
The policy includes a strong risk-based approach, the retention period allows for review during the year-end audit, and the total transaction amount has no impact on financial reporting are not the most important things for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions. These are possible factors or benefits that may influence or justify the decision, but they do not override or replace the data owner responsibilities.

**NEW QUESTION 188**
- (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 189**
- (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 193**
- (Topic 1)
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor's BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

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

**Answer:** A

**Explanation:**
When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor’s best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet, as this would provide an additional layer of security and alert the organization of any malicious traffic that bypasses or penetrates the firewall. Placing an IDS between the firewall and the demilitarized zone (DMZ), the organization’s web server, or the organization’s network would not be as effective, as it would only monitor the traffic that has already passed through the firewall. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.3

**NEW QUESTION 198**
- (Topic 1)

During the implementation of an upgraded enterprise resource planning (ERP) system, which of the following is the MOST important consideration for a go-live decision?

A. Rollback strategy
B. Test cases
C. Post-implementation review objectives
D. Business case

**Answer:** D

**Explanation:**
The most important consideration for a go-live decision when implementing an upgraded enterprise resource planning (ERP) system is the business case. The business case is the document that defines and justifies the need, value, feasibility, and risks of the project. It also outlines the expected costs, benefits, outcomes, and impacts of the project. The business case provides the basis for measuring and evaluating the success of the project. Therefore, before deciding to go live with an upgraded ERP system, it is essential to review and validate the business case to ensure that it is still relevant, accurate, realistic, and achievable.
A rollback strategy, test cases, and post-implementation review objectives are not the most important considerations for a go-live decision when implementing an upgraded ERP system. These are important elements of project planning, execution, and evaluation, but they are not sufficient to determine whether the project is worth pursuing or delivering. These elements should be aligned with and derived from the business case.

**NEW QUESTION 201**
- (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 206**
- (Topic 1)
Which of the following should an IS auditor be MOST concerned with during a post- implementation review?

A. The system does not have a maintenance plan.
B. The system contains several minor defects.
C. The system deployment was delayed by three weeks.
D. The system was over budget by 15%.

**Answer:** A

**Explanation:**
A post-implementation review (PIR) is an assessment conducted at the end of a project cycle to determine if the project was indeed successful and to identify any existing flaws in the project1. One of the main objectives of a PIR is to evaluate the outcome and functional value of a project1. Therefore, an IS auditor should be most concerned with whether the system meets the intended requirements and delivers the expected benefits to the stakeholders. A system that does not have a maintenance plan is a major risk, as it may not be able to cope with changing needs, fix errors, or prevent security breaches. A maintenance plan is essential for ensuring the system's reliability, availability, and performance in the long term2.
The other options are less critical for a PIR, as they are more related to the project management aspects than the system quality aspects. The system may contain several minor defects that do not affect its functionality or usability, and these can be resolved in future updates. The system deployment may be delayed by three weeks due to unforeseen circumstances or dependencies, but this does not necessarily mean that the system is faulty or ineffective. The system may be over budget by 15% due to various factors such as scope creep, resource constraints, or market fluctuations, but this does not imply that the system is not valuable or beneficial.
References: 1: Post-Implementation Review Best Practices - MetaPM 2: What is Post- Implementation Review in Project Management?

**NEW QUESTION 207**
- (Topic 1)
Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).
B. Determine reporting requirements for vulnerabilities.
C. Define the testing scope.
D. Obtain management consent for the testing.

**Answer:** D

**Explanation:**
The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against the organization's systems and networks, which may have legal, ethical, and operational implications. Without proper authorization from management, a penetration test may violate laws, policies, contracts, or service level agreements. Management consent also helps define the objectives, scope, and boundaries of the test, as well as the roles and responsibilities of the testers and the stakeholders. Obtaining management consent for the testing also demonstrates due care and due diligence on the part of the testers and the organization.
Executing nondisclosure agreements (NDAs), determining reporting requirements for vulnerabilities, and defining the testing scope are important steps when planning a penetration test, but they are not the first step. These steps should be done after obtaining management consent for the testing, as they depend on the approval and involvement of management and other parties.

**NEW QUESTION 210**
- (Topic 1)
Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

A. Audit cycle defined in the audit plan
B. Complexity of management's action plans
C. Recommendation from executive management
D. Residual risk from the findings of previous audits

**Answer:** D

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

**NEW QUESTION 212**
- (Topic 1)
During a new system implementation, an IS auditor has been assigned to review risk management at each milestone. The auditor finds that several risks to project benefits have not been addressed. Who should be accountable for managing these risks?

A. Enterprise risk manager
B. Project sponsor
C. Information security officer
D. Project manager

**Answer:** D

**Explanation:**
The project manager should be accountable for managing the risks to project benefits. Project benefits are the expected outcomes or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue. Project risks are uncertain events or conditions that may affect the project objectives, scope, budget, schedule, or quality. The project manager is responsible for identifying, analyzing, prioritizing, responding to, and monitoring project risks throughout the project life cycle. The other options are not accountable for managing project risks, as they have different roles and responsibilities. The enterprise risk manager is responsible for overseeing the organization's overall risk management framework and strategy, but not for managing specific project risks. The project sponsor is responsible for initiating, approving, and supporting the project, but not for managing project risks. The information security officer is responsible for ensuring that the project complies with the organization's information security policies and standards, but not for managing project risks. References:
CISA Review Manual (Digital Version), Chapter 3, Section 3.3

**NEW QUESTION 216**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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 FirstTry

* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year