Vendor: ISACA

Exam Code: CISA

Exam Name: Certified Information Systems Auditor (CISA)

Version: DEMO

QUESTION 1
An IS auditor needs to validate business logic execution by tracing through production logs. Which of the following are MOST likely to contain the appropriate entries?

A. Print server logs
B. Database logs
C. File server logs
D. Application logs

Answer: D
Explanation:
Application logs are most likely to contain entries related to business logic execution, as they record events and transactions specific to the application's operations, including user actions, process flows, and system interactions that implement business logic.

QUESTION 2
An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which of the following is the BEST recommendation?

A. Implement annual third-party audits
B. Require executive management to draft IT strategy
C. Implement key performance indicators (KPIs)
D. Benchmark organizational performance against industry peers

Answer: C
Explanation:
Key performance indicators (KPIs) are critical for improving IT governance as they provide measurable metrics to assess the performance and alignment of IT with business objectives. KPIs enable continuous monitoring and help ensure that IT initiatives support the organization's strategic goals effectively.

QUESTION 3
Which of the following approaches BEST enables an IS auditor to detect security vulnerabilities within an application?

A. Threat modelling
B. Threat intelligence
C. Concept mapping
D. Prototyping

Answer: A
Explanation:
Threat modeling is the best approach for detecting security vulnerabilities within an application. It involves identifying potential threats, vulnerabilities, and attack vectors during the design and development stages, allowing for proactive mitigation of risks and strengthening application security.

QUESTION 4
An IS auditor is planning an implementation review of a new accounting system. Which of the following is MOST important to include in this review?

A. Data conversion results
B. Benefits realization
C. Database configurations
D. System security training

Answer: A
Explanation:
In an implementation review of a new accounting system, reviewing data conversion results is critical to ensure that data from the old system has been accurately and completely migrated to the new system. Accurate data conversion is essential for the integrity and reliability of the accounting system.

QUESTION 5
Which of the following should be of GREATEST concern to an IS auditor reviewing operational log management at a large organization with a complex IT infrastructure?

A. Disk usage statistics are not logged
B. The operational logs are not using write-once-read-many media
C. A SIEM system has not been implemented
D. Retention periods vary for different types of logs being stored

Answer: B
Explanation:
The greatest concern for an IS auditor would be if operational logs are not stored on write-once-read-many (WORM) media. WORM media ensures that logs cannot be tampered with after they are written, preserving their integrity and ensuring they are reliable for investigations, compliance, and audits. This is particularly critical in large organizations with complex IT infrastructures, where log integrity is essential for identifying and addressing security incidents.

QUESTION 6
Which of the following is the MOST likely reason that an adversary would exploit security flaws in an organization's internet-connected humidity monitors?

A. To launch a ransomware attack
B. To launch a denial of service (DoS) attack
C. To launch a cryptojacking attack
D. To launch a man-in-the-middle attack

Answer: B
Explanation:
Internet-connected humidity monitors, as part of IoT devices, are often targeted for their vulnerabilities and lack of robust security. Exploiting these devices can allow an adversary to add them to a botnet, which can be used to launch Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks by overwhelming a target system with traffic. These devices typically have limited security features, making them attractive targets for such attacks.

QUESTION 7
Which of the following metrics MOST effectively measures an organization's security posture?

A. Increase in the number of external threats detected
B. Reduction in the number of undetected security events

C. Number and frequency of subsequently discovered unreported incidents
D. Time and costs spent resolving security-related incidents

Answer: B
Explanation:
A reduction in undetected security events indicates improved threat detection capabilities, which directly reflects the organization's ability to identify and mitigate risks in a timely manner. This metric provides insight into the effectiveness of security measures and the organization's overall security posture.

QUESTION 8
The use of access control lists (ACLs) is the MOST effective method to mitigate security risk for routers because they:

A. act as filters between the world and the network
B. can detect cyberattacks
C. are recommended by security standards
D. can limit Telnet and traffic from the open Internet

Answer: A
Explanation:
Access control lists (ACLs) are most effective for mitigating security risks on routers because they act as **filters**, controlling which traffic is allowed or denied based on predefined rules. This helps protect the internal network by blocking unauthorized or malicious traffic from the outside world while allowing legitimate traffic to pass.

QUESTION 9
Which of the following should be of GREATEST concern to an IS auditor reviewing controls around an artificial intelligence (AI) system in an organization?

A. Contracted developers have access to the knowledge base for maintenance purposes
B. Development of the knowledge base was outsourced to vendors
C. Basic assumptions and formulas used to develop the decision logic were not documented
D. The policy and procedure guide and its decision logic were reviewed once annually

Answer: C
Explanation:
The greatest concern for an IS auditor would be the lack of documentation for the basic assumptions and formulas used to develop the AI system's decision logic. This absence can lead to issues with transparency, accountability, and the ability to audit or validate the system's outputs. Proper documentation is critical for ensuring that the system operates as intended and that its decisions can be explained and justified if questioned.

QUESTION 10
Which of the following will have the GREATEST influence on the effectiveness of a security awareness training program?

A. Covering multiple security awareness topics in the training
B. Integrating security awareness practices into performance objectives
C. Requiring employees to take security awareness quizzes
D. Providing regularly scheduled security awareness campaigns

Answer: B
Explanation:
Integrating security awareness practices into employee performance objectives has the greatest influence on the effectiveness of a security awareness training program. It aligns individual behavior with organizational goals and reinforces the importance of security in day-to-day activities. This approach ensures that security awareness is not only understood but also practiced consistently as part of employees' responsibilities.

QUESTION 11
Which of the following should be the PRIMARY consideration when validating a data analytic algorithm that has never been used before?

A. Increasing speed and efficiency of audit procedures
B. Confirming completeness and accuracy
C. Enhancing the design of data visualization
D. Decreasing the time for data analytics execution

Answer: B
Explanation:
When validating a data analytic algorithm that has never been used before, the primary consideration should be ensuring **completeness and accuracy** of the algorithm's output. This ensures that the algorithm processes data correctly, produces reliable results, and supports decision-making or audit objectives effectively. Without validated accuracy and completeness, other factors such as speed or visualization enhancements are irrelevant.

QUESTION 12
Which of the following is the MOST important consideration when defining the recovery time objective (RTO) for a business-critical system?

A. Maximum acceptable data loss
B. Backup of data and configurations
C. Customer and business uptime requirements
D. Supporting infrastructure

Answer: C
Explanation:
The recovery time objective (RTO) defines the maximum allowable downtime for a business-critical system before significant business impact occurs. Therefore, it must be aligned with the customer and business uptime requirements, as these directly reflect the organization's operational and service-level expectations. Meeting these requirements ensures minimal disruption to business processes and customer satisfaction.

QUESTION 13
Which of the following would be of GREATEST concern to an is auditor reviewing continuous integration/continuous deployment (CI/CD) practices?

A. Dynamic application security testing (DAST) is not performed for every build
B. If all pipeline tests pass, changes are allowed to be deployed into production without manual review
C. The time between deployments has varied from four hours to two weeks

D. Critical security test failures within the pipeline do not stop production deployment

Answer: D
Explanation:
The greatest concern would be if critical security test failures within the CI/CD pipeline do not prevent deployment to production. This indicates that vulnerabilities or significant security issues could be introduced into production environments, potentially exposing the system to risks. Ensuring that critical security tests act as blocking mechanisms is essential for maintaining a secure CI/CD process.

QUESTION 14
Which of the following would be of GREATEST concern when testing an organization's controls around social engineering threats?

A. Incident handling procedures are not included in security awareness sessions
B. Staff are not aware of information asset classifications
C. Biometric authentication is not utilized
D. The intrusion detection system (IDS) is not configured properly

Answer: A
Explanation:
The greatest concern is the absence of incident handling procedures in security awareness sessions. Without proper training on how to recognize and respond to social engineering attempts, staff may fail to take appropriate actions when such threats occur. This can lead to greater vulnerability and an ineffective response to potential breaches, undermining the organization's overall security posture.

QUESTION 15
An organization intends to automate the identification of multiple transactions by the same user originating from geographically different IP addresses. Which of following techniques would MOST efficiently enable this control?

A. System snapshots
B. Log analysis
C. Audit hooks
D. IP address activity review

Answer: B
Explanation:
Log analysis is the most efficient technique for automating the identification of multiple transactions by the same user originating from geographically different IP addresses. It allows the organization to analyze patterns in real-time or batch processing by leveraging tools that process logs for anomalies such as conflicting geographic locations for the same user session.

QUESTION 16
Which of the following controls helps to reduce fraud risk associated with robotic process automation (RPA)?

A. Inclusion of robots in business impact assessments (BIAs)
B. Password rotation
C. Recertification process for robots

D. Common RPA testing framework

Answer: C
Explanation:
A recertification process for robots helps reduce fraud risk in RPA by periodically reviewing and validating the access, roles, and activities of robots to ensure they are still aligned with business requirements and security policies. This control prevents misuse, unauthorized actions, or deviations from intended processes, thereby mitigating fraud risks.

QUESTION 17
What is the purpose of hashing a document?

A. To prevent unauthorized disclosure of the contents
B. To validate the integrity of the file contents
C. To classify the file for internal use only
D. To compress the size of the file

Answer: B
Explanation:
Hashing a document generates a unique fixed-size hash value based on its contents. The purpose is to ensure the integrity of the file by enabling detection of any unauthorized changes. If the document is altered, even slightly, the hash value will change, indicating potential tampering.

QUESTION 18
An IS auditor observes that an organization's systems are being used for cryptocurrency mining on a regular basis. Which of the following is the auditor's FIRST course of action?

A. Report the incident immediately
B. Recommend changing the organization's firewall settings
C. Consult the organization's acceptable use policy
D. Require mining software to be uninstalled

Answer: C
Explanation:
The auditor's first course of action should be to consult the organization's acceptable use policy (AUP) to determine whether cryptocurrency mining is permitted or violates organizational rules. This establishes a clear understanding of the organization's stance on the activity and informs the appropriate next steps. Without reviewing the policy, it is premature to report the incident or recommend changes.

QUESTION 19
Which of the following risk scenarios is BEST mitigated through the use of a data loss prevention (DLP) tool?

A. An employee is sending company documents to an external email to increase productivity
B. A former employee retains access to an application that authenticates via single sign-on (SSO)
C. An employee uses production data in a test environment
D. An employee selects the incorrect data classification on documents

Answer: A
Explanation:

A Data Loss Prevention (DLP) tool is designed to monitor, detect, and prevent unauthorized sharing or transfer of sensitive data outside the organization. It is best suited to mitigate scenarios where employees may intentionally or unintentionally send company documents to external email addresses, which poses a risk of data leakage.

QUESTION 20
Who should be the FIRST to evaluate an audit report prior to issuing it to the project steering committee?

A. Audit committee
B. Business owner
C. Project sponsor
D. IS audit manager

Answer: D
Explanation:
The IS audit manager should be the first to evaluate an audit report before it is issued to the project steering committee. This ensures the report's accuracy, completeness, and alignment with audit objectives. The audit manager reviews findings, conclusions, and recommendations to maintain quality and professionalism in the audit deliverable.

QUESTION 21
An organization has experienced frequent of malware exploiting vulnerabilities to its network. Which of the following would be an IS auditor's BEST recommendation to address this issue?

A. Stateful inspection firewall
B. Demilitarized zone (DMZ)
C. Continuous port scanning
D. Intrusion prevention system (IPS)

Answer: D
Explanation:
An Intrusion Prevention System (IPS) is the best recommendation to address malware exploiting vulnerabilities, as it actively monitors network traffic for malicious activity and prevents it in real-time. Unlike passive solutions, an IPS can block malicious payloads and prevent vulnerabilities from being exploited, providing an effective defense against frequent malware attacks.

QUESTION 22
An IS auditor wants to gain a better understanding of an organization's selected IT operating system software. Which of the following would be MOST helpful to review?

A. IT audit reports
B. Project steering committee charter
C. Service level agreements (SLAs)
D. Enterprise architecture (EA)

Answer: D
Explanation:
The Enterprise Architecture (EA) provides a comprehensive view of the organization's IT environment, including the operating system software, its integration with other systems, and how

it supports business processes. Reviewing the EA is the most effective way for an IS auditor to understand the selected IT operating system software in the context of the organization's overall IT infrastructure.

QUESTION 23
Which of the following is the PRIMARY objective of performing quality assurance (QA) in a system development process?

A. To ensure that expected benefits have been realized
B. To ensure the developed system meets business requirements
C. To ensure the developed system integrates well with another system
D. To help determine high-level requirements for the new system

Answer: B
Explanation:
The primary objective of quality assurance (QA) in the system development process is to ensure that the system being developed adheres to the defined business requirements and specifications. QA focuses on verifying that the final product aligns with organizational needs, is free of defects, and functions as intended, thereby ensuring the project's success.

QUESTION 24
An IS auditor is planning a review of an organization’s robotic process automation (RPA) technology. Which of the following MUST be included in the audit work plan?

A. Integration architecture
B. Change management
C. Cost-benefit analysis
D. Employee training content

Answer: B
Explanation:
Change management is a critical component of any audit involving robotic process automation (RPA) technology. Since RPA systems are designed to automate processes, any changes made to the bots or workflows need to be properly managed to ensure they are aligned with business objectives and do not introduce new risks. A review of change management ensures that RPA deployments and modifications are documented, tested, and approved in a controlled manner, which helps maintain system integrity and reduces the risk of errors.

QUESTION 25
Which of the following is the BEST recommendation to prevent the skimming of debit or credit card data in point of sale (POS) systems?

A. Biometric authentication
B. Encryption
C. Chip and PIN
D. Hashing

Answer: C
Explanation:
Chip and PIN technology is the best recommendation to prevent skimming of debit or credit card data in point-of-sale (POS) systems. Chip-based cards generate a unique transaction code for

each purchase, making it extremely difficult for criminals to clone the card, even if the data is intercepted. Additionally, the use of PINs adds another layer of security, ensuring that only authorized users can complete transactions.

QUESTION 26
An IS auditor is reviewing how password resets are performed for users working remotely. Which type of documentation should be requested to understand the detailed steps required for this activity?

A. Guidelines
B. Policies
C. Procedures
D. Standards

Answer: C
Explanation:
Procedures provide detailed, step-by-step instructions for specific activities, such as password resets for remote users. They describe how tasks should be carried out in a consistent and secure manner, making them the appropriate documentation for understanding the exact steps involved in the password reset process.

QUESTION 27
Which of the following BEST supports an organization's objective of restricting the use of removable storage devices by users?

A. Data management policy
B. Updated anti-malware solutions
C. Data loss prevention (DLP)
D. Online monitoring

Answer: C
Explanation:
A Data Loss Prevention (DLP) solution is the best option to support an organization's objective of restricting the use of removable storage devices. DLP tools can enforce policies that block or control the use of USB drives and other removable media, preventing unauthorized data transfer and ensuring sensitive data remains secure.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**