Vendor: ISACA

Exam Code: CISA

Exam Name: Isaca Certified Information Systems Auditor (CISA)

Version: DEMO

QUESTION 1
An emergency power-off switch should:

A. not be in the computer room.
B. not be identified
C. be protected.
D. be illuminated.

Answer: C
Explanation:
The purpose of an emergency power-off switch is to quickly shut down power to critical systems or equipment in the event of an emergency or potential hazard. To ensure its effectiveness, the emergency power-off switch should be protected to prevent accidental or unauthorized activation.

QUESTION 2
Which of the following is the PRIMARY role of the IS auditor in an organization's information classification process?

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

Answer: B

QUESTION 3
When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

A. the project schedule.
B. quality assurance (QA) results.
C. post-implementation issues.
D. the business case

Answer: D
Explanation:
Quality assurance results are like IT checklists can be incorrect, maybe they are generic or unrelated. As IS auditor we need to understand business case first and validate QA results are correct or maybe develop our own checklist or test cases.

QUESTION 4
Which of the following is the MOST important reason for IS auditors to perform post-implementation reviews for critical IT projects?

A. To determine whether vendors should be paid for project deliverables
B. To provide the audit committee with an assessment of project team performance
C. To provide guidance on the financial return on investment (ROI) of projects
D. To determine whether the organization's objectives were met as expected

Answer: D

QUESTION 5
In a controlled application development environment, the MOST important segregation of duties should be between the person who implements changes into the production environment and the:

A. application programmer.
B. quality assurance (QA) personnel.
C. computer operator.
D. systems programmer.

Answer: A
Explanation:
Developer and deployment personnel should be segregated its main must, nothing else matters.

QUESTION 6
A small startup organization does not have the resources to implement segregation of duties. Which of the following is the MOST effective compensating control?

A. Rotation of log monitoring and analysis responsibilities
B. Additional management reviews and reconciliations
C. Mandatory vacations
D. Third-party assessments

Answer: B
Explanation:
In a small organization, where the number of employees is relatively small, job rotations may not make much sense, and they are likely to be transferred back to their original positions after a while.

QUESTION 7
When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the:

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

Answer: C

QUESTION 8
Which of the following data would be used when performing a business impact analysis (BIA)?

A. Projected impact of current business on future business
B. Expected costs for recovering the business
C. Cost of regulatory compliance
D. Cost-benefit analysis of running the current business

Answer: B

QUESTION 9
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. Number of security vulnerability patches
D. Financial impact per security event

Answer: D

QUESTION 10
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. Mobile devices are not encrypted.
B. Users are not required to sign updated acceptable use agreements.
C. The business continuity plan (BCP) was not updated.
D. Users have not been trained on the new system.

Answer: C

QUESTION 11
Which of the following security measures will reduce the risk of propagation when a cyberattack occurs?

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

Answer: C

QUESTION 12
An IS auditor notes that the previous year's disaster recovery test was not completed within the scheduled time frame due to insufficient hardware allocated by a third-party vendor. Which of the following provides the BEST evidence that adequate resources are now allocated to successfully recover the systems?

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

Answer: D

QUESTION 13
When implementing Internet Protocol security (IPsec) architecture, the servers involved in application delivery:

A. channel access only through the public-facing firewall.
B. channel access through authentication.
C. communicate via Transport Layer Security (TLS).
D. block authorized users from unauthorized activities.

Answer: B

QUESTION 14
During audit fieldwork, an IS auditor learns that employees are allowed to connect their personal devices to company-owned computers. How can the auditor BEST validate that appropriate security controls are in place to prevent data loss?

A. Verify the data loss prevention (DLP) tool is properly configured by the organization.
B. Review compliance with data loss and applicable mobile device user acceptance policies.
C. Verify employees have received appropriate mobile device security awareness training.
D. Conduct a walk-through to view results of an employee plugging in a device to transfer confidential data.

Answer: B

QUESTION 15
Management has requested a post-implementation review of a newly implemented purchasing package to determine to what extent business requirements are being met. Which of the following is MOST likely to be assessed?

A. Implementation methodology
B. Test results
C. Purchasing guidelines and policies
D. Results of live processing

Answer: D
Explanation:
The results of live processing refer to the actual operational use of the purchasing package in a live environment.

QUESTION 16
Which of the following is an advantage of using agile software development methodology over the waterfall methodology?

A. Quicker end user acceptance
B. Clearly defined business expectations
C. Quicker deliverables
D. Less funding required overall

Answer: C

QUESTION 17
In an online application, which of the following would provide the MOST information about the transaction audit trail?

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

Answer: C

QUESTION 18
On a public-key cryptosystem when there is no previous knowledge between parties, which of the following will BEST help to prevent one person from using a fictitious key to impersonate someone else?

A. Send a certificate that can be verified by a certification authority with the public key.
B. Encrypt the message containing the sender's public key, using the recipient's public key.
C. Send the public key to the recipient prior to establishing the connection.
D. Encrypt the message containing the sender's public key, using a private-key cryptosystem.

Answer: A

QUESTION 19
The IS quality assurance (QA) group is responsible for:

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

Answer: C
Explanation:
The IS quality assurance (QA) group is responsible for evaluating the quality of the information systems and ensuring that they meet established standards. This includes reviewing and testing program changes to ensure that they adhere to established standards, policies, and procedures. The QA group is also responsible for identifying and reporting any deficiencies or weaknesses in the system.

QUESTION 20
Which of the following approaches will ensure recovery time objectives (RTOs) are met for an organization's disaster recovery plan (DRP)?

A. Performing a full interruption test
B. Performing a parallel test
C. Performing a tabletop test
D. Performing a cyber-resilience test

Answer: B

QUESTION 21
Which audit approach is MOST helpful in optimizing the use of IS audit resources?

A. Agile auditing
B. Continuous auditing
C. Risk-based auditing
D. Outsourced auditing

Answer: C

QUESTION 22
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. Results of a risk assessment
B. Policies including BYOD acceptable use statements
C. Findings from prior audits
D. An inventory of personal devices to be connected to the corporate network

Answer: A
Explanation:
During the planning phase for an audit on the implementation of a bring your own device (BYOD) program, the most important input would be the results of a risk assessment. This assessment would help identify potential security risks and vulnerabilities associated with allowing personal devices onto the corporate network. Understanding the level of risk involved guides the audit's focus and helps in prioritizing the areas that need to be examined thoroughly.

QUESTION 23
An IS auditor concludes that logging and monitoring mechanisms within an organization are ineffective because central servers are not included within the central log repository. Which of the following audit procedures would have MOST likely identified this exception?

A. Comparing all servers included in the current central log repository with the listing used for the prior-year audit
B. Inspecting a sample of alerts generated from the central log repository
C. Comparing a list of all servers from the directory server against a list of all servers present in the central log repository
D. Inspecting a sample of alert settings configured in the central log repository

Answer: C

QUESTION 24
An IS auditor learns the organization has experienced several server failures in its distributed environment. Which of the following is the BEST recommendation to limit the potential impact of server failures in the future?

A. Failover power
B. Clustering

C. Parallel testing
D. Redundant pathways

Answer: B

QUESTION 25
During an ongoing audit, management requests a briefing on the findings to date. Which of the following is the IS auditor's BEST course of action?

A. Request management wait until a final report is ready for discussion.
B. Request the auditee provide management responses.
C. Review working papers with the auditee.
D. Present observations for discussion only.

Answer: D

QUESTION 26
Which of the following BEST demonstrates that IT strategy is aligned with organizational goals and objectives?

A. IT strategies are communicated to all business stakeholders.
B. Organizational strategies are communicated to the chief information officer (CIO).
C. The chief information officer (CIO) is involved in approving the organizational strategies.
D. Business stakeholders are involved in approving the IT strategy.

Answer: D

QUESTION 27
An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

A. A separate copy of the spreadsheet is routinely backed up.
B. Access to the spreadsheet is given only to those who require access.
C. There is a reconciliation process between the spreadsheet and the finance system.
D. The spreadsheet is locked down to avoid inadvertent changes.

Answer: B

QUESTION 28
Which of the following is the MOST important responsibility of user departments associated with program changes?

A. Analyzing change requests
B. Providing unit test data
C. Updating documentation to reflect latest changes
D. Approving changes before implementation

Answer: D

Explanation:
User departments play a critical role in the program change process, and their approval is crucial to ensure that changes align with business requirements, minimize disruption, and mitigate risks. By approving changes before implementation, user departments validate that the proposed changes are necessary, appropriate, and in line with the organization's objectives.

QUESTION 29
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 ad hoc.
B. SIEM reporting is customized.
C. SIEM configuration is reviewed annually.
D. The SIEM is decentralized.

Answer: D
Explanation:
A decentralized SIEM can lead to gaps in monitoring and increased complexity in managing security events. This can result in a higher risk of security incidents going undetected or not being properly addressed. Therefore, a decentralized SIEM would be of greatest concern when reviewing an organization's security information and event management solution.

QUESTION 30
A manager identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor in this scenario?

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

Answer: C

QUESTION 31
An IS auditor is evaluating the access controls for a shared customer relationship management (CRM) system. Which of the following would be the GREATEST concern?

A. Audit logging is not enabled.
B. Single sign-on is not enabled.
C. Complex passwords are not required.
D. Security baseline is not consistently applied.

Answer: A

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**