CISA Q&As

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cisa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

QUESTION 1

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

A. Restricting evidence access to professionally certified forensic investigators

B. Documenting evidence handling by personnel throughout the forensic investigation

C. Performing investigative procedures on the original hard drives rather than images of the hard drives

D. Engaging an independent third party to perform the forensic investigation

Correct Answer: B

The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation.

Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time,

location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the

investigation. References:

CISA Review Manual (Digital Version)

CISA Questions, Answers and Explanations Database

QUESTION 2

Which of the following would MOST effectively help to reduce the number of repealed incidents in an organization?

A. Testing incident response plans with a wide range of scenarios

B. Prioritizing incidents after impact assessment.

C. Linking incidents to problem management activities

D. Training incident management teams on current incident trends

Correct Answer: C

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

QUESTION 3

Which of the following is MOST critical to the success of an information security program?

A. Management\\'s commitment to information security

B. User accountability for information security

C. Alignment of information security with IT objectives

D. Integration of business and information security

Correct Answer: A

The most critical factor for the success of an information security program is management\\'s commitment to information security. Management\\'s commitment to information security means that the senior management supports, sponsors, funds, monitors and enforces the information security program within the organization. Management\\'s commitment to information security also demonstrates leadership, sets the tone and culture, and establishes the strategic direction and objectives for information security. User accountability for information security, alignment of information security with IT objectives, and integration of business and information security are also important factors for the success of an information security program, but they are not as critical as management\\'s commitment to information security, as they depend on or derive from it. References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

QUESTION 4

An IS auditor finds that confidential company data has been inadvertently leaked through social engineering. The MOST effective way to help prevent a recurrence of this issue is to implement:

A. penalties to staff for security policy breaches.

B. a third-party intrusion prevention solution.

C. a security awareness program.

D. data loss prevention (DLP) software.

Correct Answer: C

QUESTION 5

Which of the following are examples of detective controls?

A. Use of access control software and deploying encryption software

B. Source code review and echo checks in telecommunications

C. Check points in production jobs and rerun procedures

D. Continuity of operations planning and backup procedures

Correct Answer: B

QUESTION 6

To reduce operational costs, IT management plans to reduce the number of servers currently used to run business applications. Which of the following is MOST helpful to review when identifying which servers are no longer required?

A. Performance feedback from the user community

B. Contract with the server vendor

C. Server CPU usage trends

D. Mean time between failure (MTBF) of each server

Correct Answer: C

When identifying which servers are no longer required, reviewing server CPU usage trends is the most helpful approach. Monitoring the CPU usage over time provides insights into how actively a server is being utilized. Servers with

consistently low CPU usage may be candidates for consolidation or decommissioning. By analyzing CPU utilization patterns, IT management can make informed decisions about which servers can be retired without impacting performance or

availability.

References:

1.

ISACA. "Technical Guide on IT Migration Audit." 1(http://kb.icai.org/pdfs/PDFFile5b278a12a66758.27269499.pdf)

2.

Zapier. "IT audit: The ultimate guide [with checklist]." 2(https://zapier.com/blog/it-audit/)

3.

ISACA. "CISA Certification | Certified Information Systems Auditor." 3(https://www.isaca.org/credentialing/cisa)

QUESTION 7

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. Redundant pathways

B. Clustering

C. Failover power

D. Parallel testing

Correct Answer: B

Clustering is a technique that allows multiple servers to work together as a single system, providing high availability, load balancing, and fault tolerance. Clustering can limit the potential impact of server failures in a distributed environment, as it can automatically switch the workload to another server in the cluster if one server fails, without interrupting the service. Redundant pathways, failover power, and parallel testing are also useful for improving the reliability and availability of servers, but they do not directly address the issue of server failures.

QUESTION 8

Which of the following should be an IS auditor\\'s PRIMARY consideration when determining which issues to include in an audit report?

A. Professional skepticism

B. Management\\'s agreement

C. Materiality

D. Inherent risk

Correct Answer: C

Materiality is the primary consideration when determining which issues to include in an audit report, as it reflects the significance or importance of the issues to the users of the report. Materiality is a relative concept that depends on the nature, context, and amount of the issues, as well as the expectations and needs of the users. Materiality helps the auditor to prioritize the issues and communicate them clearly and concisely. References: ISACA CISA Review Manual, 27th Edition, page 256 Materiality in Auditing - AICPA Materiality in Planning and Performing an Audit - IAASB

QUESTION 9

Which of the following testing method examines internal structure or working of an application?

A. White-box testing

B. Parallel Test

C. Regression Testing

D. Pilot Testing

Correct Answer: A

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e.

black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs.

This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT).

White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system

testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemevel test. Though this method of test design can uncover many errors or problems, it has the

potential to miss unimplemented parts of the specification or missing requirements.

For your exam you should know the information below:

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically,

software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user

acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it

free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests ?usually

over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program\\'s specific logic path. However, testing all possible logical path in large

information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system\\'s "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and

user acceptance testing.

Function/validation testing ?It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems ?the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary

application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user\\'s desktop, potentially simultaneously, so it is important to test

the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following answers are incorrect:

Parallel Testing - This is the process of feeding test data into two systems ?the modified system and an alternative system and comparing the result.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests ?usually over interim platform and with only basic functionalities

Reference: CISA review manual 2014 Page number 167 Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

QUESTION 10

External audits have identified recurring exceptions in the user termination process, despite similar internal audits having reported no exceptions in the past. Which of the following is the IS auditor\\'s BEST course of action to improve the internal audit process in the future?

A. Include the user termination process in all upcoming audits.

B. Review user termination process changes.

C. Review the internal audit sampling methodology.

D. Review control self-assessment (CSA) results.

Correct Answer: C

QUESTION 11

A data breach has occurred due lo malware. Which of the following should be the FIRST course of action?

A. Notify the cyber insurance company.

B. Shut down the affected systems.

C. Quarantine the impacted systems.

D. Notify customers of the breach.

Correct Answer: C

The first course of action when a data breach has occurred due to malware is to quarantine the impacted systems. This means isolating the infected systems from the rest of the network and preventing any further communication or data

transfer with them. This can help contain the spread of the malware, limit the damage and exposure of sensitive data, and facilitate the investigation and remediation of the incident. Quarantining the impacted systems can also help preserve

the evidence and logs that may be needed for forensic analysis or legal action.

References:

[1] provides a guide on how to respond to a data breach caused by malware and recommends quarantining the impacted systems as the first step. [2] explains what is malware and how it can cause data breaches, and suggests quarantining the infected devices as a best practice. [3] describes the steps involved in quarantining a system infected by malware and the benefits of doing so.

QUESTION 12

An IS auditor discovered that a firewall has more services than needed. The IS auditor\\'s FIRST recommendation should be to:

A. ensure logging is turned on.

B. deploy a network penetration team.

C. review configurations.

D. eliminate services except for HTTPS.

Correct Answer: C

QUESTION 13

Which of the following should be the FIRST step in the incident response process for a suspected breach?

A. Inform potentially affected customers of the security breach

B. Notify business management of the security breach.

C. Research the validity of the alerted breach

D. Engage a third party to independently evaluate the alerted breach.

Correct Answer: C

The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the

incident response process, but they are not the first step.

References:

CISA Review Manual, 27th Edition, page 4251

CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

QUESTION 14

During a closing meeting, the IT manager disagrees with a valid audit finding presented by the IS auditor and requests the finding be excluded from the final report. Which of the following is the auditor\\'s BEST course of action?

A. Request that the IT manager be removed from the remaining meetings and future audits.

B. Modify the finding to include the IT manager\\'s comments and inform the audit manager of the changes.

C. Remove the finding from the report and continue presenting the remaining findings.

D. Provide the evidence which supports the finding and keep the finding in the report.

Correct Answer: D

QUESTION 15

Which of the following is the BEST way to reduce sampling risk?

A. Plan the audit in accordance with generally accepted auditing principles

B. Ensure each item has an equal chance to be selected

C. Assign experienced auditors to the sampling process.

D. Align the sampling approach with the one used by external auditors

Correct Answer: B