Vendor: Isaca

Exam Code:CISA

Exam Name: Certified Information Systems Auditor

Version: Demo

QUESTION 1

When a firewall is subjected to a probing attack, the MOST appropriate first response is for the firewall to:

A. alert the administrator.

B. break the Internet connection.

C. drop the packet

D. reject the packet.

Correct Answer: C

QUESTION 2

The PRIMARY reason for allocating sufficient time between the "go-live" phase of a new system and conducting a post-implementation review is to:

A. update project requirements and design documentation

B. increase availability of system implementation team resources

C. allow the system to stabilize in production

D. obtain sign-off on the scope of post-implementation review

Correct Answer: C

QUESTION 3

Which of the following is MOST important to define within a disaster recovery plan (DRP)?

A. Business continuity plan (BCP)

B. Test results for backup data restoration

C. A comprehensive list of disaster recovery scenarios and priorities

D. Roles and responsibilities for recovery team members

Correct Answer: D

QUESTION 4

When assessing a business case as part of a post-implementation review, the IS auditor must ensure that the:

A. feasibility of alternative project approaches has been assessed.

B. business case has not been amended since project approval.

C. quality assurance measures have been applied throughout the project.

D. amendments to the business case have been approved.

Correct Answer: D

QUESTION 5

Which of the following is a corrective control?

A. Separating equipment development testing and production

B. Verifying duplicate calculations in data processing

C. Reviewing user access rights for segregation

D. Executing emergency response plans

Correct Answer: D

QUESTION 6

Which of the following is MOST important for an IS auditor to consider during a review of the IT governance of an organization?

A. Funding allocations

B. Risk management methodology

C. Defined service levels

D. Decision making responsibilities

Correct Answer: C

QUESTION 7

Which of the following BEST facilitates the legal process in the event of an incident?

A. Right to perform e-discovery

B. Advice from legal counsel

C. Preserving the chain of custody

D. Results of a root cause analysis

Correct Answer: C

QUESTION 8

Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor s BEST recommendation for a compensating control?

A. Restrict payment authorization to senior staff members

B. Review payment transaction history.

C. Require written authorization for all payment transactions.

D. Reconcile payment transactions with invoices.

Correct Answer: C

QUESTION 9

Which of the following should be considered when examining fire suppression systems as part of a data center environmental controls review?

A. Installation manuals

B. Onsite replacement availability

C. Insurance coverage

D. Maintenance procedures

Correct Answer: D

QUESTION 10

Which of the following management decisions presents the GREATEST risk associated with data leakage?

A. There is no requirement for desktops to be encrypted

B. Staff are allowed to work remotely

C. Security awareness training is not provided to staff

D. Security policies have not been updated in the past year

Correct Answer: C

QUESTION 11

A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

A. change the password policy to improve the customer experience.

B. recommend implementing two-factor authentication.

C. research alternative secure methods of identity verification.

D. evaluate the impact of the customer\\'s experience on business revenue.

Correct Answer: C

QUESTION 12

The FIRST step in establishing an information security program is to:

A. secure organizational commitment and support

B. assess the organization\\'s compliance with regulatory requirements

C. determine the level of risk that is acceptable to senior management

D. define policies and standards that mitigate the organization\\'s risks

Correct Answer: A