Isaca

CISA

Certified Information Systems Auditor

Verified by IT Experts

Pass your exam in first attempt

Demo Questions

Topic break down

Topic	No. of Questions
Topic 1: Main Questions (240 Main Questions)	1
Topic 3: IT GOVERNANCE (111 PRACTICE QUESTION)	1
Topic 4: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT (130 PRACTICE QUESTIONS)	1
Topic 5: IT SERVICE DELIVERY AND SUPPORT (116 PRACTICE QUESTIONS)	1
Topic 6: PROTECTION OF INFORMATION ASSETS (251 PRACTICE QUESTIONS)	2
Topic 7: BUSINESS CONTINUITY AND DISASTER RECOVERY (111 PRACTICE QUESTIONS)	2
Topic 8: Mixed Questions	2

Topic 1, Main Questions (240 Main Questions)

Question No : 1 - (Topic 1)

What would an IS auditor expect to find in the console log? Choose the BEST answer.
A. Evidence of password spoofing
B. System errors
C. Evidence of data copy activities
D. Evidence of password sharing

Answer: B

Explanation: An IS auditor can expect to find system errors to be detailed in the console log.

Topic 3, IT GOVERNANCE (111 PRACTICE QUESTION)

Question No : 2 - (Topic 3)

A benefit of open system architecture is that it:
A. facilitates interoperability.
B. facilitates the integration of proprietary components.
C. will be a basis for volume discounts from equipment vendors.
D. allows for the achievement of more economies of scale for equipment.

Answer: A

Explanation:
Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

Topic 4, SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT (130 PRACTICE QUESTIONS)

Question No : 3 - (Topic 4)

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:
A. EDI trading partner agreements.
B. physical controls for terminals.
C. authentication techniques for sending and receiving messages.
D. program change control procedures.

Answer: C

Explanation:
Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

Topic 5, IT SERVICE DELIVERY AND SUPPORT (116 PRACTICE QUESTIONS)

Question No : 4 - (Topic 5)

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?
A. Session keys are dynamic
B. Private symmetric keys are used
C. Keys are static and shared
D. Source addresses are not encrypted or authenticated

Answer: A

Explanation:
WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy (WEP), which operates with static keys (same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

Topic 6, PROTECTION OF INFORMATION ASSETS (251 PRACTICE QUESTIONS)

Question No : 5 - (Topic 6)

Which of the following would be the BEST access control procedure?
A. The data owner formally authorizes access and an administrator implements the user authorization tables.
B. Authorized staff implements the user authorization tables and the data owner sanctions them.
C. The data owner and an IS manager jointly create and update the user authorization tables.
D. The data owner creates and updates the user authorization tables.

Answer: A

Explanation:
The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedurefor authorizing access.

Question No : 6 - (Topic 6)

To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's:

A. public key and then encrypt the message with the receiver's private key.
B. private key and then encrypt the message with the receiver's public key.
C. public key and then encrypt the message with the receiver's public key.
D. private key and then encrypt the message with the receiver's private key.

Answer: B

Explanation:
Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

Topic 7, BUSINESS CONTINUITY AND DISASTER RECOVERY (111 PRACTICE QUESTIONS)

Question No : 7 - (Topic 7)

Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?
A. Reviewing program code
B. Reviewing operations documentation
C. Turning off the UPS, then the power
D. Reviewing program documentation

Answer: B

Explanation:
Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

Question No : 8 - (Topic 7)

An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

A. alignment of the BCP with industry best practices.

B. results of business continuity tests performed by IS and end-user personnel.

C. off-site facility, its contents, security and environmental controls.

D. annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Answer: B

Explanation:

The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

Topic 8, Mixed Questions

Question No : 9 - (Topic 8)

Talking about application system audit, focus should always be placed on:

A. performance and controls of the system

B. the ability to limit unauthorized access and manipulation

C. input of data are processed correctly

D. output of data are processed correctly

E. changes to the system are properly authorized

F. None of the choices.

Answer: A,B,C,D,E

Explanation:

Talking about application system audit, focus should be placed on the performance and controls of the system, its ability to limit unauthorized access and manipulation, that input and output of data are processed correctly on the
system, that any changes to the system are authorized, and that users have access to the system.

Question No : 10 - (Topic 8)

Many WEP systems require a key in a relatively insecure format. What format is this?

A. binary format.

B. hexadecimal format. 128 bit format.

C. 256 bit format.

D. None of the choices.

Answer: B Explanation:

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

Many WEP systems require a key in hexadecimal format. If one chooses keys that spell words in the limited 0-9, A-F hex character set, these keys can be easily guessed.