

1. The review of router access control lists should be conducted during:
 - a. An environmental review
 - b. A network security review
 - c. A business continuity review
 - d. A data integrity review

2. During an audit of a telecommunication system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:
 - a. Encryption
 - b. Callback modems
 - c. Message authentication
 - d. Dedicated Leased lines

3. A digital signature contains a message digest to:
 - a. Show if the message has been altered after transmission
 - b. Define the encryption algorithm
 - c. Confirm the identity of the originator
 - d. Enable message transmission in a digital format

4. Digital signatures require the:
 - a. Signer to have a public key and the receiver to have a private key
 - b. Signer to have a private key and the receiver to have a public key
 - c. Signer and receiver to have a public key
 - d. Signer and receiver to have a private key

5. When using public key encryption to ensure confidentiality of data being transmitted across a network:
 - a. Both the key used to encrypt and decrypt the data are public
 - b. The key used to encrypt is private, but the key used to decrypt the data is public
 - c. The key used to encrypt is public, but the key used to decrypt the data is private
 - d. Both the key used to encrypt and decrypt the data are private

6. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?
 - a. A biometric, digitized and encrypted parameter with the customer's public key
 - b. A hash of the data that is transmitted and encrypted with the customer's private key
 - c. A hash of the data that is transmitted and encrypted with the customer's public key
 - d. The customer's scanned signature encrypted with the customer's public key

7. Email message authenticity and confidentiality is BEST achieved by signing the message using the:
 - a. Sender's private key and encrypting the message using the receiver's public key
 - b. Sender's public key and encrypting the message using the receiver's private key
 - c. Receiver's private key and encrypting the message using the sender's public key
 - d. Receiver's public key and encrypting the message using the sender's private key

8. Which of the following effectively verify the originator of a transaction?
 - a. Using a secret password between the originator and the receiver
 - b. Encrypting the transaction with the receiver's public key
 - c. Using a portable document format (PDF) to encapsulate transaction content
 - d. Digitally signing the transaction with the source's private key

9. Which of the following is the MOST effective type of antivirus software to detect an infected application?
 - a. Scanners
 - b. Active monitors
 - c. Hash-based integrity checkers
 - d. Vaccines