DOMAIN 5—PROTECTION OF INFORMATION ASSETS (27 %)

A5-1 Web application developers sometimes use hidden fields on web pages to save information about a client session. This technique is used, in some cases, to store session variables that enable persistence across web pages, such as maintaining the contents of a shopping cart on a retail web site application. The **MOST** likely web-based attack due to this practice is:

A. parameter tampering.
B. cross-site scripting.
C. cookie poisoning.
D. stealth commanding.

A is the correct answer.

Justification:

A. **Web application developers sometimes use hidden fields to save information about a client session or to submit hidden parameters, such as the language of the end user, to the underlying application. Because hidden form fields do not display in the browser, developers may feel safe passing unvalidated data in the hidden fields (to be validated later). This practice is not safe because an attacker can intercept, modify and submit requests, which can discover information or perform functions that the web developer never intended. The malicious modification of web application parameters is known as parameter tampering.**
B. Cross-site scripting involves the compromise of the web page to redirect users to content on the attacker web site. The use of hidden fields has no impact on the likelihood of a cross-site scripting attack because these fields are static content that cannot ordinarily be modified to create this type of attack. Web applications use cookies to save session state information on the client machine so that the user does not need to log on every time a page is visited.
C. Cookie poisoning refers to the interception and modification of session cookies to impersonate the user or steal logon credentials. The use of hidden fields has no relation to cookie poisoning.
D. Stealth commanding is the hijacking of a web server by the installation of unauthorized code. While the use of hidden forms may increase the risk of server compromise, the most common server exploits involve vulnerabilities of the server operating system or web server.

A5-2 Which control is the **BEST** way to ensure that the data in a file have not been changed during transmission?

A. Reasonableness check
B. Parity bits
C. Hash values
D. Check digits

C is the correct answer.

Justification:

A. A reasonableness check is used to ensure that input data is within expected values, not to ensure integrity of data transmission. Data can be changed and still pass a reasonableness test.
B. Parity bits are a weak form of data integrity checks used to detect errors in transmission, but they are not as good as using a hash.
C. **Hash values are calculated on the file and are very sensitive to any changes in the data values in the file. Thus, they are the best way to ensure that data has not changed.**
D. Check digits are used to detect an error in a numeric field such as an account number and is usually related to a transposition or transcribing error.

A5-3 The **PRIMARY** purpose of audit trails is to:

A. improve response time for users.
B. establish accountability for processed transactions.
C. improve the operational efficiency of the system.
D. provide information to auditors who wish to track transactions.

B is the correct answer.

Justification:

A. The objective of enabling software to provide audit trails is not to improve system efficiency because it often involves additional processing which may, in fact, reduce response time for users.
B. Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system.
C. Enabling audit trails involves storage and, thus, occupies disk space and may decrease operational efficiency.
D. Audit trails are used to track transactions for various purposes, not just for audit. The use of audit trails for IS auditors is valid; however, it is not the primary reason.

A5-4 Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

A. Intrusion detection systems
B. Data mining techniques
C. Stateful inspection firewalls
D. Packet filtering routers

B is the correct answer.

Justification:

A. An intrusion detection system is effective in detecting network or host-based errors but not effective in measuring fraudulent transactions.
B. Data mining is a technique used to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.
C. A firewall is an excellent tool for protecting networks and systems but not effective in detecting fraudulent transactions.
D. A packet filtering router operates at a network level and cannot see a transaction.

A5-5 Which of the following **BEST** ensures the integrity of a server's operating system?

A. Protecting the server in a secure location
B. Setting a boot password
C. Hardening the server configuration
D. Implementing activity logging

C is the correct answer.

Justification:

A. Protecting the server in a secure location is a good practice, but it does not ensure that a user will not try to exploit logical vulnerabilities and compromise the operating system (OS).
B. Setting a boot password is a good practice but does not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS.
C. **Hardening a system means to configure it in the most secure manner (install latest security patches, properly define access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and, thus, take control of the entire machine, jeopardizing the integrity of the OS.**
D. Activity logging has two weaknesses in this scenario—it is a detective control (not a preventive one), and the attacker who already gained privileged access can modify logs or disable them.

A5-6 Which of the following network components is **PRIMARILY** set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

A. Firewalls
B. Routers
C. Layer 2 switches
D. Virtual local area networks

A is the correct answer.

Justification:

A. **Firewall systems are the primary tool that enables an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls.**
B. Routers can filter packets based on parameters, such as source address but are not primarily a security tool.
C. Based on Media Access Control addresses, layer 2 switches separate traffic without determining whether it is authorized or unauthorized traffic.
D. A virtual local area network is a functionality of some switches that allows them to control traffic between different ports even though they are in the same physical local access network. Nevertheless, they do not effectively deal with authorized versus unauthorized traffic.

A5-7 An IS auditor discovers that the chief information officer (CIO) of an organization is using a wireless broadband modem using global system for mobile communications (GSM) technology. This modem is being used to connect the CIO's laptop to the corporate virtual private network when the CIO travels outside of the office. The IS auditor should:

A. do nothing because the inherent security features of GSM technology are appropriate.
B. recommend that the CIO stop using the laptop computer until encryption is enabled.
C. ensure that media access control address filtering is enabled on the network so unauthorized wireless users cannot connect.
D. suggest that two-factor authentication be used over the wireless link to prevent unauthorized communications.

A is the correct answer.

Justification:

A. **The inherent security features of global system for mobile communications (GSM) technology combined with the use of a virtual private network (VPN) are appropriate. The confidentiality of the communication on the GSM radio link is ensured by the use of encryption and the use of a VPN signifies that an encrypted session is established between the laptop and the corporate network. GSM is a global standard for cellular telecommunications that can be used for both voice and data. Currently deployed commercial GSM technology has multiple overlapping security features which prevent eavesdropping, session hijacking or unauthorized use of the GSM carrier network. While other wireless technologies such as 802.11 wireless local area network (LAN) technologies have been designed to allow the user to adjust or even disable security settings, GSM does not allow any devices to connect to the system unless all relevant security features are active and enabled.**
B. Because the chief information officer (CIO) is using a VPN it can be assumed that encryption is enabled in addition to the security features in GSM. In addition, VPNs will not allow the transfer of data for storage on the remote device (such as the CIO's laptop).
C. Media access control (MAC) filtering can be used on a wireless LAN but does not apply to a GSM network device.
D. Because the GSM network is being used rather than a wireless LAN, it is not possible to configure settings for two-factor authentication over the wireless link. However, two-factor authentication is recommended as it will better protect against unauthorized access than single factor authentication.

A5-8 Which of the following is the **BEST** way to minimize unauthorized access to unattended end-user PC systems?

A. Enforce use of a password-protected screen saver
B. Implement proximity-based authentication system
C. Terminate user session at predefined intervals
D. Adjust power management settings so the monitor screen is blank

A is the correct answer.

Justification:

A. **A password-protected screen saver with a proper time interval is the best measure to prevent unauthorized access to unattended end-user systems. It is important to ensure that users lock the workstation when they step away from the machine, which is something that could be reinforced via awareness training.**
B. There are solutions that will lock machines when users step away from their desks, and those would be suitable here; however, those tools are a more expensive solution, which would normally include the use of smart cards and extra hardware. Therefore, the use of a password-protected screen saver would be a better solution.
C. Terminating user sessions is often done for remote login (periodic re-authentication) or after a certain amount of inactivity on a web or server session. There is more risk related to leaving the workstation unlocked; therefore, this is not the correct answer.
D. Switching off the monitor would not be a solution because the monitor could simply be switched on.

A5-9 The implementation of which of the following would **MOST** effectively prevent unauthorized access to a system administration account on a web server?

A. Host intrusion detection software installed on the server
B. Password expiration and lockout policy
C. Password complexity rules
D. Two-factor authentication

D is the correct answer.

Justification:

A. Host intrusion detection software will assist in the detection of unauthorized system access but does not prevent such access.
B. While controls regarding password expiration and lockout from failed login attempts are important, two-factor authentication methods or techniques would most effectively reduce the risk of stolen or compromised credentials. Password-only based authentication may not provide adequate security.
C. While controls regarding password complexity are important, two-factor authentication methods or techniques would most effectively reduce the risk of stolen or compromised credentials.
D. **Two-factor authentication requires a user to use a password in combination with another identification factor that is not easily stolen or guessed by an attacker. Types of two-factor authentication include electronic access tokens that show one-time passwords on their display panels or biometric authentication systems.**

A5-10 An organization's IT director has approved the installation of a wireless local area network access point in a conference room for a team of consultants to access the Internet with their laptop computers. The **BEST** control to protect the corporate servers from unauthorized access is to ensure that:

A. encryption is enabled on the access point.
B. the conference room network is on a separate virtual local area network (VLAN).
C. antivirus signatures and patch levels are current on the consultants' laptops.
D. default user IDs are disabled and strong passwords are set on the corporate servers.

B is the correct answer.

Justification:

A. Enabling encryption is a good idea to prevent unauthorized network access, but it is more important to isolate the consultants from the rest of the corporate network.
B. The installation of the wireless network device presents risk to the corporate servers from both authorized and unauthorized users. A separate virtual local area network is the best solution because it ensures that both authorized and unauthorized users are prevented from gaining network access to database servers, while allowing Internet access to authorized users.
C. Antivirus signatures and patch levels are good practices but not as critical as preventing network access via access controls for the corporate servers.
D. Protecting the organization's servers through good passwords is good practice, but it is still necessary to isolate the network being used by the consultants. If the consultants can access the rest of the network, they could use password cracking tools against other corporate machines.

A5-11 The IS auditor is reviewing an organization's human resources (HR) database implementation. The IS auditor discovers that the database servers are clustered for high availability, all default database accounts have been removed and database audit logs are kept and reviewed on a weekly basis. What other area should the IS auditor check to ensure that the databases are appropriately secured?

A. Database administrators are restricted from access to HR data.
B. Database logs are encrypted.
C. Database stored procedures are encrypted.
D. Database initialization parameters are appropriate.

D is the correct answer.

Justification:

A. Database administrators would have access to all data on the server, but there is no practical control to prevent that; therefore, this would not be a concern.
B. Database audit logs normally would not contain any confidential data; therefore, encrypting the log files is not required.
C. If a stored procedure contains a security sensitive function such as encrypting data, it can be a requirement to encrypt the stored procedure. However, this is less critical than ensuring initialization parameters are correct.
D. When a database is opened, many of its configuration options are governed by initialization parameters. These parameters are usually governed by a file ("init.ora" in the case of Oracle Database Management System), which contains many settings. The system initialization parameters address many "global" database settings, including authentication, remote access and other critical security areas. To effectively audit a database implementation, the IS auditor must examine the database initialization parameters.

A5-12 An IS auditor has been asked by management to review a potentially fraudulent transaction. The **PRIMARY** focus of an IS auditor while evaluating the transaction should be to:

A. maintain impartiality while evaluating the transaction.
B. ensure that the independence of an IS auditor is maintained.
C. assure that the integrity of the evidence is maintained.
D. assess all relevant evidence for the transaction.

C is the correct answer.

Justification:
A. Although it is important for an IS auditor to be impartial, in this case it is more critical that the evidence be preserved.
B. Although it is important for an IS auditor to maintain independence, in this case it is more critical that the evidence be preserved.
C. **The IS auditor has been requested to perform an investigation to capture evidence which may be used for legal purposes, and therefore, maintaining the integrity of the evidence should be the foremost goal. Improperly handled computer evidence is subject to being ruled inadmissible in a court of law.**
D. While it is also important to assess all relevant evidence, it is more important to maintain the chain of custody, which ensures the integrity of evidence.

A5-13 A new business application has been designed in a large, complex organization and the business owner has requested that the various reports be viewed on a "need to know" basis. Which of the following access control methods would be the **BEST** method to achieve this requirement?

A. Mandatory
B. Role-based
C. Discretionary
D. Single sign-on

B is the correct answer.

Justification:
A. An access control system based on mandatory access control would be expensive, and difficult to implement and maintain in a large complex organization.
B. **Role-based access control limits access according to job roles and responsibilities and would be the best method to allow only authorized users to view reports on a need-to-know basis.**
C. Discretionary access control (DAC) is where the owner of the resources decides who should have access to that resource. Most access control systems are an implementation of DAC. This answer is not specific enough for this scenario.
D. Single sign-on is an access control technology used to manage access to multiple systems, networks and applications. This answer is not specific enough for this question.

A5-14 Which of the following is the **BEST** control to prevent the deletion of audit logs by unauthorized individuals in an organization?

A. Actions performed on log files should be tracked in a separate log.
B. Write access to audit logs should be disabled.
C. Only select personnel should have rights to view or delete audit logs.
D. Backups of audit logs should be performed periodically.

C is the correct answer.

Justification:
A. Having additional copies of log file activity would not prevent the original log files from being deleted.
B. For servers and applications to operate correctly, write access cannot be disabled.
C. **Granting access to audit logs to only system administrators and security administrators would reduce the possibility of these files being deleted.**
D. Frequent backups of audit logs would not prevent the logs from being deleted.

A5-15 A company is implementing a Dynamic Host Configuration Protocol. Given that the following conditions exist, which represents the **GREATEST** concern?

A. Most employees use laptops.
B. A packet filtering firewall is used.
C. The IP address space is smaller than the number of PCs.
D. Access to a network port is not restricted.

D is the correct answer.

Justification:
A. Dynamic Host Configuration Protocol provides convenience (an advantage) to the laptop users.
B. The existence of a firewall can be a security measure and would not normally be of concern.
C. A limited number of IP addresses can be addressed through network address translation or by increasing the number of IP addresses assigned to a particular subnet.
D. **Given physical access to a port, anyone can connect to the internal network. This would allow individuals to connect that were not authorized to be on the corporate network.**

A5-16 Which of the following is an effective preventive control to ensure that a database administrator (DBA) complies with the custodianship of the enterprise's data?

A. Exception reports
B. Segregation of duties
C. Review of access logs and activities
D. Management supervision

B is the correct answer.

Justification:
A. Exception reports are detective controls used to indicate when the activities of the database administrator (DBA) were performed without authorization.
B. **Adequate segregation of duties (SoD) is a preventative control that can restrict the activities of the DBA to those that have been authorized by the data owners. SoD can restrict what a DBA can do by requiring more than one person to participate to complete a task.**
C. Reviews of access logs are used to detect the activities performed by the DBA.
D. Management supervision of DBA activities is used to detect which DBA activities were not authorized.

A5-17 An employee has received a digital photo frame as an gift and has connected it to his/her work PC to transfer digital photos. The **PRIMARY** risk that this scenario introduces is that:

A. the photo frame storage media could be used to steal corporate data.
B. the drivers for the photo frame may be incompatible and crash the user's PC.
C. the employee may bring inappropriate photographs into the office.
D. the photo frame could be infected with malware.

D is the correct answer.

Justification:

A. Although any storage device could be used to steal data, the damage caused by malware could be widespread and severe for the enterprise, which is the more significant risk.
B. Although device drivers may be incompatible and crash the user's PC, the damage caused by malware could be widespread and severe for the enterprise.
C. Although inappropriate content could result, the damage caused by malware could be widespread and severe for the enterprise.
D. Any storage device can be a vehicle for infecting other computers with malware. There are several examples where it has been discovered that some devices are infected in the factory during the manufacturing process and controls should exist to prohibit employees from connecting any storage media devices to their company-issued PCs.

A5-18 An organization discovers that the computer of the chief financial officer has been infected with malware that includes a keystroke logger and a rootkit. The **FIRST** action to take would be to:

A. Contact the appropriate law enforcement authorities to begin an investigation.
B. Immediately ensure that no additional data are compromised.
C. Disconnect the PC from the network.
D. Update the antivirus signature on the pc to ensure that the malware or virus is detected and removed.

C is the correct answer.

Justification:

A. Although contacting law enforcement may be needed, the first step would be to halt data flow by disconnecting the computer from the network.
B. The first step is to disconnect the computer from the network thus ensuring that no additional data are compromised. and then, using proper forensic techniques, capture the information stored in temporary files, network connection information, programs loaded into memory and other information on the machine.
C. The most important task is to prevent further data compromise and preserve evidence by disconnecting the computer from the network.
D. Preserve the machine in a forensically sound condition and do not make any changes to it except to disconnect it from the network. Otherwise evidence would be destroyed by powering off the PC or updating the software on the PC. Information stored in temporary files, network connection information, programs loaded into memory, and other information may be lost.

A5-19 The IS auditor is reviewing findings from a prior IS audit of a hospital. One finding indicates that the organization was using email to communicate sensitive patient issues. The IT manager indicates that to address this finding, the organization has implemented digital signatures for all email users. What should the IS auditor's response be?

A. Digital signatures are not adequate to protect confidentiality.
B. Digital signatures are adequate to protect confidentiality.
C. The IS auditor should gather more information about the specific implementation.
D. The IS auditor should recommend implementation of digital watermarking for secure email.

A is the correct answer.

Justification:

A. **Digital signatures are designed to provide authentication and nonrepudiation for email and other transmissions but are not adequate for confidentiality. This implementation is not adequate to address the prior-year's finding.**
B. Digital signatures do not encrypt message contents, which means that an attacker who intercepts a message can read the message because the data are in plaintext.
C. Although gathering additional information is always a good step before drawing a conclusion on a finding, in this case the implemented solution simply does not provide confidentiality.
D. Digital watermarking is used to protect intellectual property rights for documents rather than to protect the confidentiality of email.

A5-20 Which of the following line media would provide the **BEST** security for a telecommunication network?

A. Broadband network digital transmission
B. Baseband network
C. Dialup
D. Dedicated lines

D is the correct answer.

Justification:

A. The secure use of broadband communications is subject to whether the network is shared with other users, the data are encrypted and the risk of network interruption.
B. A baseband network is one that is usually shared with many other users and requires encryption of traffic but still may allow some traffic analysis by an attacker.
C. A dial-up line is fairly secure because it is a private connection, but it is too slow to be considered for most commercial applications today.
D. **Dedicated lines are set apart for a particular user or organization. Because there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.**

A5-21 To ensure that an organization is complying with privacy requirements, an IS auditor should **FIRST** review:

A. the IT infrastructure.
B. organizational policies, standards and procedures.
C. legal and regulatory requirements.
D. adherence to organizational policies, standards and procedures.

C is the correct answer.

Justification:

A. To comply with requirements, the IS auditor must first know what the requirements are. They can vary from one jurisdiction to another. The IT infrastructure is related to the implementation of the requirements.
B. The policies of the organization are subject to the legal requirements and should be checked for compliance after the legal requirements are reviewed.
C. **To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.**
D. Checking for compliance is only done after the IS auditor is assured that the policies, standards and procedures are aligned with the legal requirements.

A5-22 A human resources company offers wireless Internet access to its guests, after authenticating with a generic user ID and password. The generic ID and password are requested from the reception desk. Which of the following controls **BEST** addresses the situation?

A. The password for the wireless network is changed on a weekly basis.
B. A stateful inspection firewall is used between the public wireless and company networks.
C. The public wireless network is physically segregated from the company network.
D. An intrusion detection system is deployed within the wireless network.

C is the correct answer.

Justification:

A. Changing the password for the wireless network does not secure against unauthorized access to the company network, especially because a guest could gain access to the wireless local area network at any time prior to the weekly password change interval.
B. A stateful inspection firewall will screen all packets from the wireless network into the company network; however, the configuration of the firewall would need to be audited and firewall compromises, although unlikely, are possible.
C. **Keeping the wireless network physically separate from the company network is the best way to secure the company network from intrusion.**
D. An intrusion detection system will detect intrusions but will not prevent unauthorized individuals from accessing the network.

A5-23 When reviewing the implementation of a local area network, an IS auditor should **FIRST** review the:

A. node list.
B. acceptance test report.
C. network diagram.
D. users list.

C is the correct answer.

Justification:
A. Verification of nodes from the node list would follow the review of the network diagram.
B. The review of the acceptance test report would follow the verification of nodes from the node list.
C. **To properly review a local area network implementation, an IS auditor should first verify the network diagram to identify risk or single points of failure.**
D. The users list would be reviewed after the acceptance test report.

A5-24 An IS auditor discovers that the configuration settings for password controls are more stringent for business users than for IT developers. Which of the following is the **BEST** action for the IS auditor to take?

A. Determine whether this is a policy violation and document it.
B. Document the observation as an exception.
C. Recommend that all password configuration settings be identical.
D. Recommend that logs of IT developer access are reviewed periodically.

A is the correct answer.

Justification:
A. **If the policy documents the purpose and approval for different procedures, then an IS auditor only needs to document observations and tests as to whether the procedures are followed.**
B. This condition would not be considered an exception if procedures are followed according to approved policies.
C. There may be valid reasons for these settings to be different; therefore, the auditor would not normally recommend changes before researching company policies and procedures.
D. While reviewing logs may be a good compensating control, the more important course of action would be to determine if policies are being followed.

A5-25 An organization is developing a new web-based application to process orders from customers. Which of the following security measures should be taken to protect this application from hackers?

A. Ensure that ports 80 and 443 are blocked at the firewall.
B. Inspect file and access permissions on all servers to ensure that all files have read-only access.
C. Perform a web application security review.
D. Make sure that only the IP addresses of existing customers are allowed through the firewall.

C is the correct answer.

Justification:
A. Port 80 must be open for a web application to work and port 443 for a Secured Hypertext Transmission Protocol to operate.
B. For customer orders to be placed, some data must be saved to the server. No customer orders could be placed on a read-only server.
C. **Performing a web application security review is a necessary effort that would uncover security vulnerabilities that could be exploited by hackers.**
D. Restricting IP addresses might be appropriate for some types of web applications but is not the best solution because a new customer could not place an order until the firewall rules were changed to allow the customer to connect.

A5-26 Which of the following types of penetration tests simulates a real attack and is used to test incident handling and response capability of the target?

A. Blind testing
B. Targeted testing
C. Double-blind testing
D. External testing

C is the correct answer.

Justification:

A. Blind testing is also known as black-box testing. This refers to a test where the penetration tester is not given any information and is forced to rely on publicly available information. This test simulates a real attack, except that the target organization is aware of the test being conducted.
B. Targeted testing is also known as white-box testing. This refers to a test where the penetration tester is provided with information and the target organization is also aware of the testing activities. In some cases, the tester is also provided with a limited-privilege account to be used as a starting point.
C. **Double-blind testing is also known as zero-knowledge testing. This refers to a test where the penetration tester is not given any information and the target organization is not given any warning—both parties are "blind" to the test. This is the best scenario for testing response capability because the target will react as if the attack were real.**
D. External testing refers to a test where an external penetration tester launches attacks on the target's network perimeter from outside the target network (typically from the Internet).

A5-27 An organization has requested that an IS auditor provide a recommendation to enhance the security and reliability of its Voice-over Internet Protocol (VoIP) system and data traffic. Which of the following would meet this objective?

A. VoIP infrastructure needs to be segregated using virtual local area networks.
B. Buffers need to be introduced at the VoIP endpoints.
C. Ensure that end-to-end encryption is enabled in the VoIP system.
D. Ensure that emergency backup power is available for all parts of the VoIP infrastructure.

A is the correct answer.

Justification:

A. **Segregating the Voice-over Internet Protocol (VoIP) traffic using virtual local area networks (VLANs) would best protect the VoIP infrastructure from network-based attacks, potential eavesdropping and network traffic issues (which would help to ensure uptime).**
B. The use of packet buffers at VoIP endpoints is a method to maintain call quality, not a security method.
C. Encryption is used when VoIP calls use the Internet (not the local LAN) for transport because the assumption is that the physical security of the building as well as the Ethernet switch and VLAN security is adequate.
D. The design of the network and the proper implementation of VLANs are more critical than ensuring that all devices are protected by emergency power.

A5-28 During a review of intrusion detection logs, an IS auditor notices traffic coming from the Internet, which appears to originate from the internal IP address of the company payroll server. Which of the following malicious activities would **MOST** likely cause this type of result?

A. A denial-of-service attack
B. Spoofing
C. Port scanning
D. A man-in-the-middle attack

B is the correct answer.

Justification:

A. A denial-of-service attack is designed to limit the availability of a resource and is characterized by a high number of requests that require response from the resource (usually a web site). The target spends so many resources responding to the attack requests that legitimate requests are not serviced. These attacks are most commonly launched from networks of compromised computers (botnets) and may involve attacks from multiple computers at once.

B. Spoofing is a form of impersonation where one computer tries to take on the identity of another computer. When an attack originates from the external network but uses an internal network address, the attacker is most likely trying to bypass firewalls and other network security controls by impersonating (or spoofing) the payroll server's internal network address. By impersonating the payroll server, the attacker may be able to access sensitive internal resources.

C. Port scanning is a reconnaissance technique that is designed to gather information about a target before a more active attack. Port scanning might be used to determine the internal address of the payroll server but would not normally create a log entry that indicated external traffic from an internal server address.

D. A man-in-the-middle attack is a form of active eavesdropping where the attacker intercepts a computerized conversation between two parties and then allows the conversation to continue by relaying the appropriate data to both parties, while simultaneously monitoring the same data passing through the attacker's conduit. This type of attack would not register as an attack originating from the payroll server, but instead it might be designed to hijack an authorized connection between a workstation and the payroll server.

A5-29 An IS auditor is reviewing an organization's information security policy, which requires encryption of all data placed on universal serial bus (USB) drives. The policy also requires that a specific encryption algorithm be used. Which of the following algorithms would provide the greatest assurance that data placed on USB drives is protected from unauthorized disclosure?

A. Data Encryption Standard
B. Message digest 5
C. Advanced Encryption Standard
D. Secure Shell

C is the correct answer.

Justification:

A. Data Encryption Standard (DES) is susceptible to brute force attacks and has been broken publicly; therefore, it does not provide assurance that data encrypted using DES will be protected from unauthorized disclosure.
B. Message digest 5 (MD5) is an algorithm used to generate a one-way hash of data (a fixed- length value) to test and verify data integrity. MD5 does not encrypt data but puts data through a mathematical process that cannot be reversed. As a result, MD5 could not be used to encrypt data on a universal serial bus (USB) drive.
C. Advanced Encryption Standard (AES) provides the strongest encryption of all of the choices listed and would provide the greatest assurance that data are protected. Recovering data encrypted with AES is considered computationally infeasible and so AES is the best choice for encrypting sensitive data.
D. Secure Shell (SSH) is a protocol that is used to establish a secure, encrypted, command-line shell session, typically for remote logon. Although SSH encrypts data transmitted during a session, SSH cannot encrypt data at rest, including data on USB drives. As a result, SSH is not appropriate for this scenario.

A5-30 During an IS audit of a global organization, the IS auditor discovers that the organization uses Voice-over Internet Protocol over the Internet as the sole means of voice connectivity among all offices. Which of the following presents the **MOST** significant risk for the organization's VoIP infrastructure?

A. Network equipment failure
B. Distributed denial-of-service attack
C. Premium-rate fraud (toll fraud)
D. Social engineering attack

B is the correct answer.

Justification:

A. The use of Voice-over Internet Protocol does not introduce any unique risk with respect to equipment failure, and redundancy can be used to address network failure.
B. A distributed denial-of-service (DDoS) attack would potentially disrupt the organization's ability to communicate among its offices and have the highest impact. In a traditional voice network, a DDoS attack would only affect the data network, not voice communications.
C. Toll fraud occurs when someone compromises the phone system and makes unauthorized long-distance calls. While toll fraud may cost the business money, the more severe risk would be the disruption of service.
D. Social engineering, which involves gathering sensitive information to launch an attack, can be exercised over any kind of telephony.

A5-31 Which of the following is the **MOST** effective control for restricting access to unauthorized Internet sites in an organization?

A. Routing outbound Internet traffic through a content-filtering proxy server
B. Routing inbound Internet traffic through a reverse proxy server
C. Implementing a firewall with appropriate access rules
D. Deploying client software utilities that block inappropriate content

A is the correct answer.

Justification:

A. A content-filtering proxy server will effectively monitor user access to Internet sites and block access to unauthorized web sites.
B. When a client web browser makes a request to an Internet site, those requests are outbound from the corporate network. A reverse proxy server is used to allow secure remote connection to a corporate site, not to control employee web access.
C. A firewall exists to block unauthorized inbound and outbound network traffic. Some firewalls can be used to block or allow access to certain sites, but the term firewall is generic—there are many types of firewalls, and this is not the best answer.
D. While client software utilities do exist to block inappropriate content, installing and maintaining additional software on a large number of PCs is less effective than controlling the access from a single, centralized proxy server.

A5-32 An internal audit function is reviewing an internally developed common gateway interface script for a web application. The IS auditor discovers that the script was not reviewed and tested by the quality control function. Which of the following types of risk is of **GREATEST** concern?

A. System unavailability
B. Exposure to malware
C. Unauthorized access
D. System integrity

C is the correct answer.

Justification:

A. While untested common gateway interfaces (CGIs) can cause the end-user web application to be compromised, this is not likely to make the system unavailable to other users.
B. Untested CGI scripts do not inherently lead to malware exposures.
C. Untested CGIs can have security weaknesses that allow unauthorized access to private systems because CGIs are typically executed on publicly available Internet servers.
D. While untested CGIs can cause the end-user web application to be compromised, this is not likely to significantly impact system integrity.

A5-33 An IS auditor is conducting a postimplementation review of an enterprise's network. Which of the following findings would be of **MOST** concern?

A. Wireless mobile devices are not password-protected.
B. Default passwords are not changed when installing network devices.
C. An outbound web proxy does not exist.
D. All communication links do not use encryption.

B is the correct answer.

Justification:
A. While mobile devices that are not password-protected would be a risk, it would not be as significant as unsecured network devices.
B. **The most significant risk in this case would be if the factory default passwords are not changed on critical network equipment. This could allow anyone to change the configurations of network equipment.**
C. The use of a web proxy is a good practice but may not be required depending on the enterprise.
D. Encryption is a good control for data security but is not appropriate to use for all communication links due to cost and complexity.

A5-34 An IS auditor is reviewing a third-party agreement for a new cloud-based accounting service provider. Which of the following considerations is the **MOST** important with regard to the privacy of the accounting data?

A. Data retention, backup and recovery
B. Return or destruction of information
C. Network and intrusion detection
D. A patch management process

B is the correct answer.

Justification:
A. Data retention, backup and recovery are important controls; however, they do not guarantee data privacy.
B. **When reviewing a third-party agreement, the most important consideration with regard to the privacy of the data is the clause concerning the return or secure destruction of information at the end of the contract.**
C. Network and intrusion detection are helpful when securing the data, but on their own, they do not guarantee data privacy stored at a third-party provider.
D. A patch management process helps secure servers and may prohibit unauthorized disclosure of data; however, it does not affect the privacy of the data.

A5-35 Which of the following is the **MOST** effective control when granting temporary access to vendors?

A. Vendor access corresponds to the service level agreement.
B User accounts are created with expiration dates and are based on services provided.
C. Administrator access is provided for a limited period.
D. User IDs are deleted when the work is completed.

B is the correct answer.

Justification:

A. The service level agreement may have a provision for providing access, but this is not a control; it would merely define the need for access.
B. The most effective control is to ensure that the granting of temporary access is based on services to be provided and that there is an expiration date (automated is best) associated with each unique ID. The use of an identity management system enforces temporary and permanent access for users, at the same time ensuring proper accounting of their activities.
C. Vendors may require administrator access for a limited period during the time of service. However, it is important to ensure that the level of access granted is set according to least privilege and that access during this period is monitored.
D. Deleting these user IDs after the work is completed is necessary, but if not automated, the deletion could be overlooked. The access should only be granted at the level of work required.

A5-36 During a logical access controls review, an IS auditor observes that user accounts are shared. The **GREATEST** risk resulting from this situation is that:

A. an unauthorized user may use the ID to gain access.
B. user access management is time consuming.
C. passwords are easily guessed.
D. user accountability may not be established.

D is the correct answer.

Justification:

A. The ability of unauthorized users to use a shared ID is more likely than of an individual ID—but the misuse of another person's ID is always a risk.
B. Using shared IDs would not pose an increased risk due to work effort required for managing access.
C. Shared user IDs do not necessarily have easily guessed passwords.
D. The use of a user ID by more than one individual precludes knowing who, in fact, used that ID to access a system; therefore, it is impossible to hold anyone accountable.

A5-37 An IS auditor is assessing a biometric system used to protect physical access to a data center containing regulated data. Which of the following observations is the **GREATEST** concern to the auditor?

A. Administrative access to the biometric scanners or the access control system is permitted over a virtual private network.
B. Biometric scanners are not installed in restricted areas.
C. Data transmitted between the biometric scanners and the access control system do not use a securely encrypted tunnel.
D. Biometric system risk analysis was last conducted three years ago.

C is the correct answer.

Justification:

A. Generally, virtual private network software provides a secure tunnel so that remote administration functions can be performed. This is not a concern.
B. Biometric scanners are best located in restricted areas to prevent tampering, but video surveillance is an acceptable mitigating control. The greatest concern is lack of a securely encrypted tunnel between the scanners and the access control system.
C. Data transmitted between the biometric scanners and the access control system should use a securely encrypted tunnel to protect the confidentially of the biometric data.
D. The biometric risk analysis should be reperformed periodically, but an analysis performed three years ago is not necessarily a cause for concern.

A5-38 When auditing a role-based access control system, the IS auditor noticed that some IT security employees have system administrator privileges on some servers, which allows them to modify or delete transaction logs. Which would be the **BEST** recommendation that the IS auditor should make?

A. Ensure that these employees are adequately supervised.
B. Ensure that backups of the transaction logs are retained.
C. Implement controls to detect the changes.
D. Write transaction logs in real time to Write Once and Read Many drives.

D is the correct answer.

Justification:

A. IT security employees cannot be supervised in the traditional sense unless the supervisor were to monitor each keystroke entered on a workstation, which is obviously not a realistic option.
B. Retaining backups of the transaction logs does not prevent the files from unauthorized modification prior to backup.
C. The log files themselves are the main evidence that an unauthorized change was made, which is a sufficient detective control. Protecting the log files from modification requires preventive controls such as securely writing the logs.
D. Allowing IT security employees access to transaction logs is often unavoidable because having system administrator privileges is required for them to do their job. The best control in this case, to avoid unauthorized modifications of transaction logs, is to write the transaction logs to WORM drive media in real time. It is important to note that simply backing up the transaction logs to tape is not adequate because data could be modified prior (typically at night) to the daily backup job execution.

A5-39 During an IS audit of a bank, the IS auditor is assessing whether the enterprise properly manages staff member access to the operating system. The IS auditor should determine whether the enterprise performs:

A. periodic review of user activity logs.
B. verification of user authorization at the field level.
C. review of data communication access activity logs.
D. periodic review of changing data files.

A is the correct answer.

Justification:

A. **General operating system access control functions include logging user activities, events, etc. Reviewing these logs may identify users performing activities that should not have been permitted.**
B. Verification of user authorization at the field level is a database- and/or an application-level access control function and not applicable to an operating system.
C. Review of data communication access activity logs is a network control feature.
D. Periodic review of changing data files is related to a change control process.

A5-40 An IS auditor performing an audit of the newly installed Voice-over Internet Protocol system was inspecting the wiring closets on each floor of a building. What would be the **GREATEST** concern?

A. The local area network (LAN) switches are not connected to uninterruptible power supply units.
B. Network cabling is disorganized and not properly labeled.
C. The telephones are using the same cable used for LAN connections.
D. The wiring closet also contains power lines and breaker panels.

A is the correct answer.

Justification:

A. **Voice-over Internet Protocol (VoIP) telephone systems use standard network cabling and typically each telephone gets power over the network cable (power over Ethernet) from the wiring closet where the network switch is installed. If the local area network switches do not have backup power, the phones will lose power if there is a utility interruption and potentially not be able to make emergency calls.**
B. While improper cabling can create reliability issues, the more critical issue in this case would be the lack of power protection.
C. An advantage of VoIP telephone systems is that they use the same cable types and even network switches as standard PC network connections. Therefore, this would not be a concern.
D. As long as the power and telephone equipment are separated, this would not be a significant risk.

A5-41 When reviewing an organization's logical access security to its remote systems, which of the following would be of **GREATEST** concern to an IS auditor?

A. Passwords are shared.
B. Unencrypted passwords are used.
C. Redundant logon IDs exist.
D. Third-party users possess administrator access.

B is the correct answer.

Justification:
A. The passwords should not be shared, but this is less important than ensuring that the password files are encrypted.
B. When evaluating the technical aspects of logical security, unencrypted passwords represent the greatest risk because it would be assumed that remote access would be over an untrusted network where passwords could be discovered.
C. Checking for the redundancy of logon IDs is essential but is less important than ensuring that the passwords are encrypted.
D. There may be business requirements such as the use of contractors that requires them to have system access, so this may not be a concern.

A5-42 During an IS risk assessment of a health care organization regarding protected health care information (PHI), an IS auditor interviews IS management. Which of the following findings from the interviews would be of **MOST** concern to the IS auditor?

A. The organization does not encrypt all of its outgoing email messages.
B. Staff have to type "[PHI]" in the subject field of email messages to be encrypted.
C. An individual's computer screen saver function is disabled.
D. Server configuration requires the user to change the password annually.

B is the correct answer.

Justification:
A. Encrypting all outgoing email is expensive and is not common business practice.
B. There will always be human-error risk that staff members forget to type certain words in the subject field. The organization should have automated encryption set up for outgoing email for employees working with protected health care information (PHI) to protect sensitive information.
C. Disabling the screen saver function increases the risk that sensitive data can be exposed to other employees; however, the risk is not as great as exposing the data to unauthorized individuals outside the organization.
D. While changing the password annually is a concern, the risk is not as great as exposing the data to unauthorized individuals outside the organization.

A5-43 Which of the following is the responsibility of information asset owners?

A. Implementation of information security within applications
B. Assignment of criticality levels to data
C. Implementation of access rules to data and programs
D. Provision of physical and logical security for data

B is the correct answer.

Justification:

A. Implementation of information security within an application is the responsibility of the data custodians based on the requirements set by the data owner.
B. It is the responsibility of owners to define the criticality (and sensitivity) levels of information assets.
C. Implementation of access rules is a responsibility of data custodians based on the requirements set by the data owner.
D. Provision of physical and logical security for data is the responsibility of the security administrator.

A5-44 An IS auditor reviewing a network log discovers that an employee ran elevated commands on their PC by invoking the task scheduler to launch restricted applications. This is an example what type of attack?

A. A race condition
B. A privilege escalation
C. A buffer overflow
D. An impersonation

B is the correct answer.

Justification:

A. A race condition exploit involves the timing of two events and an action that causes one event to happen later than expected. The scenario given is not an example of a race condition exploit.
B. A privilege escalation is a type of attack where higher-level system authority is obtained by various methods. In this example, the task scheduler service runs with administrator permissions, and a security flaw allows programs launched by the scheduler to run at the same permission level.
C. Buffer overflows involve applications of actions that take advantage of a defect in the way an application or system uses memory. By overloading the memory storage mechanism, the system will perform in unexpected ways. The scenario given is not an example of a buffer overflow exploit.
D. Impersonation attacks involve an error in the identification of a privileged user. The scenario given is not an example of this exploit.

A5-45 An IS auditor is reviewing an organization to ensure that evidence related to a data breach case is preserved. Which of the following choices would be of **MOST** concern to the IS auditor?

A. End users are not aware of incident reporting procedures.
B. Log servers are not on a separate network.
C. Backups are not performed consistently.
D. There is no chain of custody policy.

D is the correct answer.

Justification:

A. End users should be made aware of incident reporting procedures, but this is not likely to affect data integrity related to the breach. The IS auditor would be more concerned that the organization's policy exists and provides for proper evidence handling.
B. Having log servers segregated on a separate network might be a good idea because ensuring the integrity of log server data is important. However, it is more critical to ensure that the chain of custody policy is in place.
C. While not having valid backups would be a concern, the more important concern would be a lack of a chain of custody policy. Data breach evidence is not normally retrieved from backups.
D. Organizations should have a policy in place that directs employees to follow certain procedures when collecting evidence that may be used in a court of law. Chain of custody involves documentation of how digital evidence is acquired, processed, handled, stored and protected, and who handled the evidence and why. If there is no policy in place, it is unlikely that employees will ensure that the chain of custody is maintained during any data breach investigation.

A5-46 An IS auditor is reviewing access controls for a manufacturing organization. During the review, the IS auditor discovers that data owners have the ability to change access controls for a low-risk application. The **BEST** course of action for the IS auditor is to:

A. recommend that mandatory access control be implemented.
B. report this as a finding to upper management
C. report this to the data owners to determine whether it is an exception.
D. not report this issue because discretionary access controls are in place.

D is the correct answer.

Justification:

A. Recommending mandatory access control is not correct because it is more appropriate for data owners to have discretionary access controls (DAC) in a low-risk application.
B. The use of DAC may not be an exception and, until confirmed, should not be reported as an issue.
C. While an IS auditor may consult with data owners regarding whether this access is allowed normally, the IS auditor should not rely on the auditee to determine whether this is an issue.
D. DAC allows data owners to modify access, which is a normal procedure and is a characteristic of DAC.

A5-47 Electromagnetic emissions from a terminal represent a risk because they:

A. could damage or erase nearby storage media.
B. can disrupt processor functions.
C. could have adverse health effects on personnel.
D. can be detected and displayed.

D is the correct answer.

Justification:

A. While a strong magnetic field can erase certain storage media, normally terminals are designed to limit these emissions; therefore, this is not normally a concern.
B. Electromagnetic emissions should not cause disruption of central processing units.
C. Most electromagnetic emissions are low level and do not pose a significant health risk.
D. Emissions can be detected by sophisticated equipment and displayed, thus giving unauthorized persons access to data. TEMPEST is a term referring to the investigation and study of compromising emanations of unintentional intelligence-bearing signals that, if intercepted and analyzed, may reveal their contents.

A5-48 Security administration procedures require read-only access to:

A. access control tables.
B. security log files.
C. logging options.
D. user profiles.

B is the correct answer.

Justification:

A. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements.
B. Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities.
C. Logging options require write access to allow the administrator to update the way the transactions and user activities are monitored, captured, stored, processed and reported.
D. The security administrator is often responsible for user-facing issues such as managing user roles, profiles and settings. This requires the administrator to have more than read-only access.

A5-49 With the help of a security officer, granting access to data is the responsibility of:

A. data owners.
B. programmers.
C. system analysts.
D. librarians.

A is the correct answer.

Justification:

A. **Data owners are responsible for the access to and use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners' approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).**
B. Programmers will develop the access control software that will regulate the ways that users can access the data (update, read, delete, etc.), but the programmers do not have responsibility for determining who gets access to data.
C. Systems analysts work with the owners and programmers to design access controls according to the rules set by the owners.
D. The librarians enforce the access control procedures they have been given but do not determine who gets access.

A5-50 The **FIRST** step in data classification is to:

A. establish ownership.
B. perform a criticality analysis.
C. define access rules.
D. create a data dictionary.

A is the correct answer.

Justification:

A. **Data classification is necessary to define access rules based on a need-to-do and need-to- know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification.**
B. A criticality analysis is required to determine the appropriate levels of protection of data, according to the data classification.
C. Access rules are set up dependent on the data classification.
D. Input for a data dictionary is prepared from the results of the data classification process.

A5-51 During the review of a biometrics system operation, an IS auditor should **FIRST** review the stage of:

A. enrollment.
B. identification.
C. verification.
D. storage.

A is the correct answer.

Justification:

A. The users of a biometric device must first be enrolled in the device.
B. The device captures a physical or behavioral image of the human, identifies the unique features and uses an algorithm to convert them into a string of numbers stored as a template to be used in the matching processes.
C. A user applying for access will be verified against the stored enrolled value.
D. The biometric stores sensitive personal information, so the storage must be secure.

A5-52 A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineering.
B. sniffers.
C. back doors.
D. Trojan horses.

A is the correct answer.

Justification:

A. Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal data.
B. A sniffer is a computer tool to monitor the traffic in networks.
C. Back doors are computer programs left by hackers to exploit vulnerabilities.
D. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually malicious in nature.

A5-53 The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trail.
B. the security administrator has read-only rights to the audit file.
C. date and time stamps are recorded when an action occurs.
D. users can amend audit trail records when correcting system errors.

D is the correct answer.

Justification:

A. An audit trail must record the identity of the person or process involved in the logged activity to establish accountability.
B. Restricting the administrator to read-only access will protect the audit file from alteration.
C. Data and time stamps should be recorded in the logs to enable the reconstruction and correlation of events on multiple systems.
D. An audit trail is not effective if the details in it can be amended.

A5-54 While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's **NEXT** step?

A. Observe the response mechanism.
B. Clear the virus from the network.
C. Inform appropriate personnel immediately.
D. Ensure deletion of the virus.

C is the correct answer.

Justification:
A. Observing the response mechanism should be done after informing appropriate personnel. This will enable an IS auditor to examine the actual workability and effectiveness of the response system.
B. The IS auditor is neither authorized nor capable in most cases of removing the virus from the network.
C. **The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response.**
D. An IS auditor should not make changes to the system being audited; ensuring the deletion of the virus is a management responsibility.

A5-55 The implementation of access controls **FIRST** requires:

A. a classification of IS resources.
B. the labeling of IS resources.
C. the creation of an access control list.
D. an inventory of IS resources.

D is the correct answer.

Justification:
A. The first step in implementing access controls is an inventory of IS resources, which is the basis for classification.
B. Labeling resources cannot be done without first determining the resources' classifications.
C. The access control list would not be done without a meaningful classification of resources.
D. **The first step in implementing access controls is an inventory of IS resources, which is the basis for establishing ownership and classification.**

A5-56 Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls to consecutively check the incoming network traffic
B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic
C. Lack of physical signs on the outside of a computer center building
D. Using two firewalls in parallel to check different types of incoming traffic

B is the correct answer.

Justification:
A. Use of two firewalls would not represent an effective defense in-depth strategy because the same attack could circumvent both devices. By using two different products, the probability of both products having the same vulnerabilities is diminished.
B. **Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense.**
C. Having no physical signs on the outside of a computer center building is a single security measure known as security by obscurity.
D. Using two firewalls in parallel to check different types of incoming traffic provides redundancy but is only a single security mechanism and, therefore, no different than having a single firewall checking all traffic.

A5-57 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 approves 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.

A is the correct answer.

Justification:

A. **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 at the direction of the owner.**
B. The owner sets the rules and conditions for access. It is best to obtain approval before implementing the tables.
C. The data owner may consult with the IS manager to set out access control rules, but the responsibility for appropriate access remains with the data owner. The IT department should set up the access control tables at the direction of the owner.
D. The data owner would not usually manage updates to the authorization tables.

A5-58 Which of the following would **MOST** effectively reduce social engineering incidents?

A. Security awareness training
B. Increased physical security measures
C. Email monitoring policy
D. Intrusion detection systems

A is the correct answer.

Justification:

A. **Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents.**
B. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the incident.
C. An email monitoring policy informs users that all email in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders.
D. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

A5-59 An information security policy stating that "the display of passwords must be masked or suppressed" addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

C is the correct answer.

Justification:

A. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person.
B. This policy only refers to "the display of passwords," not dumpster diving (looking through an organization's trash for valuable information).
C. **If a password is displayed on a monitor, any person or camera nearby could look over the shoulder of the user to obtain the password.**
D. Impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

A5-60 To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be changed.
B. passwords are periodically changed.
C. an automated password management tool be used.
D. security awareness training is delivered.

C is the correct answer.

Justification:

A. The policy is appropriate and does not require change. Changing the policy would not ensure compliance.
B. Having a requirement to periodically change passwords is good practice and should be in the password policy.
C. **The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing his/her old password for a designated period of time.**
D. Security awareness training would not enforce compliance.

A5-61 An IS auditor reviewing digital rights management applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures
B. Hashing
C. Parsing
D. Steganography

D is the correct answer.

Justification:

A. Digitalized signatures are the scans of a signature (not the same as a digital signature) and not related to digital rights management.
B. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography.
C. Parsing is the process of splitting up a continuous stream of characters for analytical purposes and is widely applied in the design of programming languages or in data entry editing.
D. Steganography is a technique for concealing the existence of messages or information within another message. An increasingly important steganographical technique is digital watermarking, which hides data within data (e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities).

A5-62 The information security policy that states "each individual must have his/her badge read at every controlled door" addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

A is the correct answer.

Justification:

A. Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger. If every employee must have their badge read at every controlled door, no unauthorized person could enter the sensitive area.
B. Shoulder surfing (looking over the shoulder of a person to view sensitive information on a screen or desk) would not be prevented by the implementation of this policy.
C. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method.
D. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

A5-63 Which of the following presents an inherent risk with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

C is the correct answer.

Justification:

A. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights (e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions). This could be prevented by encrypting the message.
B. Viruses are malicious program code inserted into another executable code that can self-replicate and spread from computer to computer via sharing of computer disks, transfer of logic over telecommunication lines or direct contact with an infected machine. Antivirus software can be used to protect the computer against viruses.
C. **Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling.**
D. The shutdown of an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

A5-64 The **MOST** important difference between hashing and encryption is that hashing:

A. is irreversible.
B. output is the same length as the original message.
C. is concerned with integrity and security.
D. is the same at the sending and receiving end.

A is the correct answer.

Justification:

A. **Hashing works one way—by applying a hashing algorithm to a message, a message hash/digest is created. If the same hashing algorithm is applied to the message digest, it will not result in the original message. As such, hashing is irreversible, while encryption is reversible. This is the basic difference between hashing and encryption.**
B. Hashing creates a fixed-length output that is usually smaller than the original message, and encryption creates an output that is usually the same length as the original message.
C. Hashing is used to verify the integrity of the message and does not address security. The same hashing algorithm is used at the sending and receiving ends to generate and verify the message hash/digest.
D. Encryption may use different keys or a reverse process at the sending and receiving ends to encrypt and decrypt.

A5-65 Which of the following cryptography options would increase overhead/cost?

A. The encryption is symmetric rather than asymmetric.
B. A long asymmetric encryption key is used.
C. The hash is encrypted rather than the message.
D. A secret key is used.

B is the correct answer.

Justification:

A. An asymmetric algorithm requires more processing time than symmetric algorithms.
B. Computer processing time is increased for longer asymmetric encryption keys, and the increase may be disproportionate. For example, one benchmark showed that doubling the length of an RSA key from 512 bits to 1,024 bits caused the decrypt time to increase nearly six-fold.
C. A hash is usually shorter than the original message; therefore, a smaller overhead is required if the hash is encrypted rather than the message.
D. Use of a secret key, as a symmetric encryption key, is generally small and used for the purpose of encrypting user data.

A5-66 The **MOST** important factor in planning a black box penetration test is:

A. the documentation of the planned testing procedure.
B. a realistic evaluation of the environment architecture to determine scope.
C. knowledge by the management staff of the client organization.
D. scheduling and deciding on the timed length of the test.

C is the correct answer.

Justification:

A. A penetration test should be carefully planned and executed, but the most important factor is proper approvals.
B. In a black box penetration test, the environment is not known to the testing organization.
C. Black box penetration testing assumes no prior knowledge of the infrastructure to be tested. Testers simulate an attack from someone who is unfamiliar with the system. It is important to have management knowledge of the proceedings so that if the test is identified by the monitoring systems, the legality of the actions can be determined quickly.
D. A test must be scheduled so as to minimize the risk of affecting critical operations; however, this is part of working with the management of the organization.

A5-67 An organization allows for the use of universal serial bus drives to transfer operational data between offices. Which of the following is the **GREATEST** risk associated with the use of these devices?

A. Files are not backed up
B. Theft of the devices
C. Use of the devices for personal purposes
D. Introduction of malware into the network

B is the correct answer.

Justification:
A. While this is a risk, theft of an unencrypted device is a greater risk.
B. Because universal serial bus (USB) drives tend to be small, they are susceptible to theft or loss. This represents the greatest risk to the organization.
C. Use of USB drives for personal purposes is a violation of company policy; however, this is not the greatest risk.
D. Good general IT controls will include the scanning of USB drives for malware once they are inserted in a computer. The risk of malware in an otherwise robust environment is not as great as the risk of loss or theft.

A5-68 When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be **MOST** concerned with:

A. analysis.
B. evaluation.
C. preservation.
D. disclosure.

C is the correct answer.

Justification:
A. Analysis is important but not the primary concern related to evidence in a forensic investigation.
B. Evaluation is important but not the primary concern related to evidence in a forensic investigation.
C. Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when investigating. Failure to properly preserve the evidence could jeopardize the admissibility of the evidence in legal proceedings.
D. Disclosure is important but not of primary concern to the IS auditor in a forensic investigation.

A5-69 A certificate authority (CA) can delegate the processes of:

A. revocation and suspension of a subscriber's certificate.
B. generation and distribution of the CA public key.
C. establishing a link between the requesting entity and its public key.
D. issuing and distributing subscriber certificates.

C is the correct answer.

Justification:
A. Revocation and suspension of the subscriber certificate are functions of the subscriber certificate life cycle management, which the certificate authority (CA) must perform.
B. Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.
C. Establishing a link between the requesting entity and its public key is a function of a registration authority. This may or may not be performed by a CA; therefore, this function can be delegated.
D. Issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform.

A5-70 Which of the following results in a denial-of-service attack?

A. Brute force attack
B. Ping of death
C. Leapfrog attack
D. Negative acknowledgment attack

B is the correct answer.

Justification:

A. A brute force attack is typically a text attack that exhausts all possible key combinations used against encryption keys or passwords.
B. The use of Ping with a packet size higher than 65 KB and no fragmentation flag on will cause a denial of service.
C. A leapfrog attack, the act of telneting through one or more hosts to preclude a trace, makes use of user ID and password information obtained illicitly from one host to compromise another host.
D. A negative acknowledgment is a penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, leaving the system in an unprotected state during such interrupts.

A5-71 Which of the following is an advantage of elliptic curve encryption over RSA encryption?

A. Computation speed
B. Ability to support digital signatures
C. Simpler key distribution
D. Message integrity controls

A is the correct answer.

Justification:

A. The main advantage of elliptic curve encryption (ECC) over RSA encryption is its computation speed. This is due in part to the use of much smaller keys in the ECC algorithm than in RSA.
B. Both encryption methods support digital signatures.
C. Both encryption methods are used for public key encryption and distribution.
D. Both ECC and RSA offer message integrity controls.

A5-72 Which of the following would be the **BEST** overall control for an Internet business looking for confidentiality, reliability and integrity of data?

A. Secure Sockets Layer
B. Intrusion detection system
C. Public key infrastructure
D. Virtual private network

A is the correct answer.

Justification:

A. Secure Sockets Layer (SSL) is used for many ecommerce applications to set up a secure channel for communications providing confidentiality through a combination of public and symmetric key encryption and integrity through hash message authentication code.
B. An intrusion detection system will log network activity but is not used for protecting traffic over the Internet.
C. Public key infrastructure is used in conjunction with SSL or for securing communications such as ecommerce and email.
D. A virtual private network (VPN) is a generic term for a communications tunnel that can provide confidentiality, integrity and authentication (reliability). A VPN can operate at different levels of the Open Systems Interconnection stack and may not always be used in conjunction with encryption. SSL can be called a type of VPN.

A5-73 Which of the following preventive controls **BEST** helps secure a web application?

A. Password masking
B. Developer training
C. Use of encryption
D. Vulnerability testing

B is the correct answer.

Justification:

A. Password masking is a necessary preventive control but is not the best way to secure an application.
B. Of the given choices, teaching developers to write secure code is the best way to secure a web application.
C. Encryption will protect data but is not sufficient to secure an application because other flaws in coding could compromise the application and data. Ensuring that applications are designed in a secure way is the best way to secure an application. This is accomplished by ensuring that developers are adequately educated on secure coding practices.
D. Vulnerability testing can help to ensure the security of web applications; however, the best preventive control is developer education because building secure applications from the start is more effective.

A5-74 Which of the following antivirus software implementation strategies would be the **MOST** effective in an interconnected corporate network?

A. Server-based antivirus software
B. Enterprise-based antivirus software
C. Workstation-based antivirus software
D. Perimeter-based antivirus software

B is the correct answer.

Justification:

A. An effective antivirus solution must be a combination of server-, network- and perimeter-based scanning and protection.
B. An important means of controlling the spread of viruses is to deploy an enterprisewide antivirus solution that will monitor and analyze traffic at many points. This provides a layered defense model that is more likely to detect malware regardless of how it comes into the organization—through a universal serial bus (USB) or portable storage, a network, an infected download or malicious web application.
C. Only checking for a virus on workstations would not be adequate because malware can infect many network devices or servers as well.
D. Because malware can enter an organization through many different methods, only checking for malware at the perimeter is not enough to protect the organization.

A5-75 Which of the following would be of **MOST** concern to an IS auditor reviewing a virtual private network implementation? Computers on the network that are located:

A. on the enterprise's internal network.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

C is the correct answer.

Justification:

A. On an enterprise's internal network, there should be security policies and controls in place to detect and halt an outside attack that uses an internal machine as a staging platform.
B. Computers at the backup site are subject to the corporate security policy and, therefore, are not high-risk computers.
C. **One risk of a virtual private network implementation is the chance of allowing high-risk computers onto the enterprise's network. All machines that are allowed onto the virtual network should be subject to the same security policy. Home computers are least subject to the corporate security policies and, therefore, are high-risk computers. Once a computer is hacked and "owned," any network that trusts that computer is at risk. Implementation and adherence to corporate security policy is easier when all computers on the network are on the enterprise's campus.**
D. Computers on the network that are at the enterprise's remote offices, perhaps with different IS and security employees who have different ideas about security, are riskier than computers in the main office or backup site, but obviously less risky than home computers.

A5-76 The **PRIMARY** reason for using digital signatures is to ensure data:

A. confidentiality.
B. integrity.
C. availability.
D. correctness.

B is the correct answer.

Justification:

A. A digital signature does not, in itself, address message confidentiality.
B. **Digital signatures provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered. A digital signature provides for message integrity, nonrepudiation and proof of origin.**
C. Availability is not related to digital signatures.
D. In general, correctness is not related to digital signatures. A digital signature guarantee data integrity, however cannot ensure correctness of signed data.

A5-77 Which of the following is an example of a passive cybersecurity attack?

A. Traffic analysis
B. Masquerading
C. Denial-of-service
D. Email spoofing

A is the correct answer.

Justification:

A. **Cybersecurity threats/vulnerabilities are divided into passive and active attacks. A passive attack is one that monitors or captures network traffic but does not in any way modify, insert or delete the traffic. Examples of passive attacks include network analysis, eavesdropping and traffic analysis.**
B. Because masquerading alters the data by modifying the origin, it is an active attack.
C. Because a denial-of–service attack floods the network with traffic or sends malformed packets over the network, it is an active attack.
D. Because email spoofing alters the email header, it is an active attack.

A5-78 An IS auditor is reviewing security incident management procedures for the company. Which of the following choices is the **MOST** important consideration?

A. Chain of custody of electronic evidence
B. System breach notification procedures
C. Escalation procedures to external agencies
D. Procedures to recover lost data

A is the correct answer.

Justification:

A. **The preservation of evidence is the most important consideration in regard to security incident management. If data and evidence are not collected properly, valuable information could be lost and would not be admissible in a court of law should the company decide to pursue litigation.**
B. System breach notification is an important aspect and, in many cases, may even be required by laws and regulations; however, the security incident may not be a breach and the notification procedure might not apply.
C. Escalation procedures to external agencies such as the local police or special agencies dealing in cybercrime are important. However, without proper chain of custody procedures, vital evidence may be lost and would not be admissible in a court of law should the company decide to pursue litigation.
D. While having procedures in place to recover lost data is important, it is critical to ensure that evidence is protected to ensure follow-up and investigation.

A5-79 An accuracy measure for a biometric system is:

A. system response time.
B. registration time.
C. input file size.
D. false-acceptance rate.

D is the correct answer.

Justification:

A. An important consideration in the implementation of biometrics is the time required to process a user. If the system is too slow then it will impact productivity and lead to frustration. However, this is not an accuracy measure.
B. The registration time is a measure of the effort taken to enroll a user in the system. This is not an accuracy measure.
C. The file size to retain biometric information varies depending on the type of biometric solution selected. This is not an accuracy measure.
D. Three main accuracy measures are used for a biometric solution: false-rejection rate (FRR), cross-error rate (CER) and false-acceptance rate (FAR). FRR is a measure of how often valid individuals are rejected. FAR is a measure of how often invalid individuals are accepted. CER is a measure of when the false-rejection rate equals the false-acceptance rate.

A5-80 An IS auditor evaluating logical access controls should **FIRST**:

A. document the controls applied to the potential access paths to the system.
B. test controls over the access paths to determine if they are functional.
C. evaluate the security environment in relation to written policies and practices.
D. obtain an understanding of the security risk to information processing.

D is the correct answer.

Justification:

A. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness of the controls and is based on the risk to the system that necessitates the controls.
B. The third step is to test the access paths—to determine if the controls are functioning.
C. It is only after the risk is determined and the controls documented that the IS auditor can evaluate the security environment to assess its adequacy through review of the written policies, observation of practices and comparison of them to appropriate security good practices.
D. When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risk facing information processing by reviewing relevant documentation, by inquiries, and conducting a risk assessment. This is necessary so that the IS auditor can ensure the controls are adequate to address risk.

A5-81 Which of the following is the **MOST** secure way to remove data from obsolete magnetic tapes during a disposal?

A. Overwriting the tapes
B. Initializing the tape labels
C. Degaussing the tapes
D. Erasing the tapes

C is the correct answer.

Justification:

A. Overwriting the tapes is a good practice, but if the tapes have contained sensitive information then it is necessary to degauss them.
B. Initializing the tape labels would not remove the data on the tape and could lead to compromise of the data on the tape.
C. **The best way to handle obsolete magnetic tapes is to degauss them. Degaussing is the application of a coercive magnetic force to the tape media. This action leaves a very low residue of magnetic induction, essentially erasing the data completely from the tapes.**
D. Erasing the tapes will make the data unreadable except for sophisticated attacks; therefore, tapes containing sensitive data should be degaussed.

A5-82 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.

B is the correct answer.

Justification:

A. Environmental reviews examine physical security such as power and physical access. They do not require a review of the router access control lists.
B. **Network security reviews include reviewing router access control lists, port scanning, internal and external connections to the system, etc.**
C. Business continuity reviews ensure the business continuity plan is up to date, adequate to protect the organization and tested, and do not require a review of the router access control lists.
D. Data integrity reviews validate data accuracy and protect from improper alterations, but do not require a review of the router access control lists.

A5-83 Which of the following components is responsible for the collection of data in an intrusion detection system?

A. Analyzer
B. Administration console
C. User interface
D. Sensor

D is the correct answer.

Justification:

A. Analyzers receive input from sensors and determine the presence of and type of intrusive activity.
B. An administration console is the management interface component of an intrusion detection system (IDS).
C. A user interface allows the administrators to interact with the IDS.
D. Sensors are responsible for collecting data. Sensors may be attached to a network, server or other location and may gather data from many points for later analysis.

A5-84 Which of the following is the **MOST** significant function of a corporate public key infrastructure and certificate authority employing X.509 digital certificates?

A. It provides the public/private key set for the encryption and signature services used by email and file space.
B. It binds a digital certificate and its public key to an individual subscriber's identity.
C. It provides the authoritative source for employee identity and personal details.
D. It provides the authoritative authentication source for object access.

B is the correct answer.

Justification:

A. While some email applications depend on public key infrastructure (PKI)-issued certificates for nonrepudiation, the purpose of PKI is to provide authentication of the individual and link an individual with their private key. The certificate authority (CA) does not ordinarily create the user's private key.
B. PKI is primarily used to gain assurance that protected data or services originated from a legitimate source. The process to ensure the validity of the subscriber identity by linking to the digital certificate/public key is strict and rigorous.
C. Personal details are not stored in or provided by components in the PKI.
D. Authentication services within operating systems and applications may be built on PKI-issued certificates, but PKI does not provide authentication services for object access.

A5-85 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.

A is the correct answer.

Justification:

A. The message digest is calculated and included in a digital signature to prove that the message has not been altered. The message digest sent with the message should have the same value as the recalculation of the digest of the received message.
B. The message digest does not define the algorithm; it is there to ensure integrity.
C. The message digest does not confirm the identity of the user; it is there to ensure integrity.
D. The message digest does not enable the transmission in digital format; it is there to ensure integrity.

A5-86 Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to ecommerce?

A. Registration authority
B. Certificate authority
C. Certification revocation list
D. Certification practice statement

B is the correct answer.

Justification:

A. A registration authority is an optional entity that is responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the certificate authority (CA).
B. The CA maintains a directory of digital certificates for the reference of those receiving them. It manages the certificate life cycle, including certificate directory maintenance and certificate revocation list (CRL) maintenance and publication.
C. A CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. A certificate that is put on a CRL can no longer be trusted.
D. A certification practice statement is a detailed set of rules governing the certificate authority's operations.

A5-87 A Transmission Control Protocol/Internet Protocol (TCP/IP)-based environment is exposed to the Internet. Which of the following **BEST** ensures that complete encryption and authentication protocols exist for protecting information while transmitted?

A. Work is completed in tunnel mode with IP security.
B. A digital signature with RSA has been implemented.
C. Digital certificates with RSA are being used.
D. Work is being completed in TCP services.

A is the correct answer.

Justification:

A. Tunnel mode with Internet Protocol (IP) security provides encryption and authentication of the complete IP package. To accomplish this, the authentication header and encapsulating security payload services can be nested. This is known as IP Security.
B. A digital signature with RSA provides authentication and integrity but not confidentiality.
C. Digital certificates with RSA provide authentication and integrity but do not provide encryption.
D. Transmission Control Protocol services do not provide encryption and authentication.

A5-88 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.

B is the correct answer.

Justification:

A. If a sender encrypts a message with a public key, it will provide confidential transmission to the receiver with the private key.
B. Digital signatures are intended to verify to a recipient the integrity of the data and the identity of the sender. The digital signature standard is based on the sender encrypting a digest of the message with their private key and the receiver validating the message with the public key.
C. Asymmetric key cryptography always works with key pairs. Therefore, a message encrypted with a public key could only be opened with a private key.
D. If both the sender and receiver have a private key there would be no way to validate the digital signature.

A5-89 The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

A. data integrity.
B. authentication.
C. nonrepudiation.
D. replay protection.

C is the correct answer.

Justification:

A. Data integrity refers to changes in the plaintext message that would result in the recipient failing to compute the same message hash.
B. Because only the claimed sender has the private key used to create the digital signature, authentication ensures that the message has been sent by the claimed sender.
C. Integrity, authentication, nonrepudiation and replay protection are all features of a digital signature. Nonrepudiation ensures that the claimed sender cannot later deny generating and sending the message.
D. Replay protection is a method that a recipient can use to check that the message was not intercepted and re-sent (replayed).

A5-90 During the collection of forensic evidence, which of the following actions would **MOST** likely result in the destruction or corruption of evidence on a compromised system?

A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network

C is the correct answer.

Justification:

A. Copying the memory contents is a normal forensics procedure where possible. Done carefully, it will not corrupt the evidence.
B. Proper forensics procedures require creating two copies of the images of the system for analysis. Hash values ensure that the copies are accurate.
C. **Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory.**
D. When investigating a system, it is recommended to disconnect it from the network to minimize external infection or access.

A5-91 An IS auditor is reviewing Secure Sockets Layer enabled web sites for the company. Which of the following choices would be the **HIGHEST** risk?

A. Expired digital certificates
B. Self-signed digital certificates
C. Using the same digital certificate for multiple web sites
D. Using 56-bit digital certificates

B is the correct answer.

Justification:

A. An expired certificate leads to blocked access to the web site leading to unwanted downtime. However, there is no loss of data. Therefore, the comparative risk is lower.
B. **Self-signed digital certificates are not signed by a certificate authority (CA) and can be created by anyone. Thus, they can be used by attackers to impersonate a web site, which may lead to data theft or perpetrate a man-in-the-middle attack.**
C. Using the same digital certificate is not a significant risk. Wildcard digital certificates may be used for multiple subdomain web sites.
D. 56-bit digital certificates may be needed to connect with older versions of operating systems (OSs) or browsers. While they have a lower strength than 128-bit or 256-bit digital certificates, the comparative risk of a self-signed certificate is higher.

A5-92 Which of the following controls would **BEST** detect intrusion?

A. User IDs and user privileges are granted through authorized procedures.
B. Automatic logoff is used when a workstation is inactive for a particular period of time.
C. Automatic logoff of the system occurs after a specified number of unsuccessful attempts.
D. Unsuccessful logon attempts are monitored by the security administrator.

D is the correct answer.

Justification:
A. User IDs and the granting of user privileges define a policy. This is a type of administrative or managerial control that may prevent intrusion but would not detect it.
B. Automatic logoff is a method of preventing access through unattended or inactive terminals but is not a detective control.
C. Unsuccessful attempts to log on are a method for preventing intrusion, not detecting it.
D. Intrusion is detected by the active monitoring and review of unsuccessful logon attempts.

A5-93 Which of the following is the **BEST** control over a guest wireless ID that is given to vendor staff?

A. Assignment of a renewable user ID which expires daily
B. A write-once log to monitor the vendor's activities on the system
C. Use of a user ID format similar to that used by employees
D. Ensuring that wireless network encryption is configured properly

A is the correct answer.

Justification:
A. A renewable user ID which expires daily would be a good control because it would ensure that wireless access will automatically terminate daily and cannot be used without authorization.
B. While it is recommended to monitor vendor activities while vendor staff are on the system, this is a detective control and thus is not as strong as a preventive control.
C. The user ID format does not change the overall security of the wireless connection.
D. Controls related to the encryption of the wireless network are important; however, the access to that network is a more critical issue.

A5-94 An IS auditor performing a telecommunication access control review should be concerned **PRIMARILY** with the:

A. maintenance of access logs of usage of various system resources.
B. authorization and authentication of the user prior to granting access to system resources.
C. adequate protection of stored data on servers by encryption or other means.
D. accountability system and the ability to identify any terminal accessing system resources.

B is the correct answer.

Justification:
A. The maintenance of access logs of usage of system resources is a detective control. A preventive control should be used first.
B. The authorization and authentication of users before granting them access to system resources (networks, servers, applications, etc.) is the most significant aspect in a telecommunication access control review because it is a preventive control. Weak controls at this level can affect all other aspects of security.
C. The adequate protection of data being stored on servers by encryption or other means is a method of protecting stored information and is not a network access issue.
D. The accountability system and the ability to identify any terminal accessing system resources deal with controlling access through the identification of a terminal or device attempting to connect to the network. This is called node authentication and is not as good as authenticating the user sitting at that node.

A5-95 An IS auditor suspects an incident is occurring while an audit is being performed on a financial system. What should the IS auditor do **FIRST**?

A. Request that the system be shut down to preserve evidence.
B. Report the incident to management.
C. Ask for immediate suspension of the suspect accounts.
D. Investigate the source and nature of the incident.

B is the correct answer.

Justification:
A. The IS auditor should follow the incident response process of the organization. The auditor is not authorized to shut the system down.
B. Reporting the suspected incident to management will help initiate the incident response process, which is the most appropriate action. Management is responsible for making decisions regarding the appropriate response. It is not the IS auditor's role to respond to incidents during an audit.
C. The IS auditor is not authorized to lead the investigation or to suspend user accounts. The auditor should report the incident to management.
D. Management is responsible to set up and follow an incident management plan; that is not the responsibility of the IS auditor.

A5-96 When using public key encryption to secure 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.

C is the correct answer.

Justification:
A. The public and private keys always work as a pair—if a public key is used to encrypt a message, the corresponding private key MUST be used to decrypt the message.
B. If the message is encrypted with a private key, that will provide proof of origin but not message security or confidentiality.
C. Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.
D. Using two private keys would not be possible with asymmetric encryption.

A5-97 The technique used to ensure security in virtual private networks is called:

A. data encapsulation.
B. data wrapping.
C. data transformation.
D. data hashing.

A is the correct answer.

Justification:
A. Encapsulation, or tunneling, is a technique used to encrypt the traffic payload so that it can be securely transmitted over an insecure network.
B. Wrapping is used where the original packet is wrapped in another packet but is not directly related to security.
C. To transform or change the state of the communication would not be used for security.
D. Hashing is used in virtual private networks to ensure message integrity.

A5-98 During an audit of a telecommunications 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.

A is the correct answer.

Justification:
A. Encryption of data is the most secure method of protecting confidential data from exposure.
B. A callback system is used to ensure that a user is only logging in from a known location. It is not effective to protect the transmitted data from interception.
C. Message authentication is used to prove message integrity and source but not confidentiality.
D. It is more difficult to intercept traffic traversing a dedicated leased line than it is to intercept data on a shared network, but the only way to really protect the confidentiality of data is to encrypt it.

A5-99 An Internet-based attack using password sniffing can:

A. enable one party to act as if they are another party.
B. cause modification to the contents of certain transactions.
C. be used to gain access to systems containing proprietary information.
D. result in major problems with billing systems and transaction processing agreements.

C is the correct answer.

Justification:
A. Spoofing attacks can be used to enable one party to act as if they are another party.
B. Data modification attacks can be used to modify the contents of certain transactions.
C. Password sniffing attacks can be used to gain access to systems on which proprietary information is stored.
D. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

A5-100 Which of the following controls would be the **MOST** comprehensive in a remote access network with multiple and diverse subsystems?

A. Proxy server
B. Firewall installation
C. Demilitarized zone
D. Virtual private network

D is the correct answer.

Justification:
A. A proxy server is a type of firewall installation used as an intermediary to filter and control traffic between internal and external parties.
B. While firewall installations are the primary line of defense, they would need to have encryption and a virtual private network (VPN) to secure remote access traffic.
C. A demilitarized zone (DMZ) is an isolated network used to permit outsiders to access certain corporate information in a semi-trusted environment. The DMZ may host a web server or other external facing services. Traffic to a DMZ is not usually encrypted unless it is terminating on a VPN located in the DMZ.
D. The best way to secure remote access is through the use of encrypted VPNs. This would allow remote users a secure connection to the main systems.

A5-101 During an audit of an enterprise that is dedicated to ecommerce, 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, digitalized 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

B is the correct answer.

Justification:

A. Biometrics are not used in digital signatures or public key encryption.
B. The calculation of a hash, or digest, of the data that are transmitted, and its encryption require the private key of the client (sender) and is called a signature of the message, or digital signature. The receiver hashes the received message and compares the hash they compute with the received hash, after the digital signature has been decrypted with the sender's public key. If the hash values are the same, the conclusion would be that there is integrity in the data that have arrived, and the origin is authenticated. The concept of encrypting the hash with the private key of the originator provides nonrepudiation because it can only be decrypted with their public key, and the private key would not be known to the recipient. Simply put, in a key-pair situation, anything that can be decrypted by a sender's public key must have been encrypted with their private key, so they must have been the sender (i.e., nonrepudiation).
C. It would not be correct to encrypt the hash with the customer's public key because then the recipient would need access to the customer's private key to decrypt the digital signature.
D. A scan of the customer's signature would be known as a digitized signature, not a digital signature, and would be of little or no value in this scenario.

A5-102 When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

A. Wiring and schematic diagram
B. Users' lists and responsibilities
C. Application lists and their details
D. Backup and recovery procedures

A is the correct answer.

Justification:

A. The wiring and schematic diagram of the network is necessary to carry out a network audit. The IS auditor needs to know what equipment, configuration and addressing is used on the network to perform an audit of the network setup.
B. When performing an audit of network setup, the users' lists would not be of value.
C. Application lists are not required to audit network configuration.
D. Backup and recovery procedures are important but not as important as knowing the network layout.

A5-103 Which of the following should an IS auditor be **MOST** concerned about in a financial application?

A. Programmers have access to source code in user acceptance testing environment.
B. Secondary controls are documented for identified role conflicts.
C. The information security officer does not authorize all application changes.
D. Programmers have access to the production database.

D is the correct answer.

Justification:

A. Programmers who have access to application source code are not of concern to the IS auditor because programmers need access to source code to do their jobs. User acceptance testing (UAT) environment is a separate from production environment, changes cannot be moved into production environment without prior authorization.
B. When segregation of duties conflicts are identified, secondary controls should be in place to mitigate risk. While the IS auditor reviews secondary controls, in this case the greater concern is programmers having access to the production database.
C. The information security officer is not likely to authorize all application changes; therefore, this is not a concern for an IS auditor.
D. Programmers who have access to the production database are considered to be a segregation of duties conflict.

A5-104 Which of the following is the **MAIN** reason an organization should have an incident response plan? The plan helps to:

A. ensure prompt communication of adverse events to relevant management.
B. contain costs related to maintaining disaster recovery plan capabilities.
C. ensure that customers are promptly notified of issues such as security breaches.
D. minimize the duration and impact of system outages and security incidents.

D is the correct answer.

Justification:

A. Incident response plans generally deal with a wide range of possible issues. While it is important to have a proper communication of adverse event within the organization, the primary objective is to reduce impact of incidents.
B. An effective incident response plan could minimize damage to the organization, which minimizes costs, but the main purpose of the incident response plan is to minimize damage. Possible damage could include nonfinancial metrics, such as damage to a company's reputation.
C. While an incident response plan includes elements such as when and how to contact customers about a significant incident, the primary purpose of the plan is to minimize the impact.
D. An incident response plan helps minimize the impact of an incident because it provides a controlled response to incidents. The phases of the plan include planning, detection, evaluation, containment, eradication, escalation, response, recovery, reporting, postincident review and a review of lessons learned.

A5-105 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.

A is the correct answer.

Justification:

A. **By signing the message with the sender's private key, the receiver can verify its authenticity using the sender's public key. Encrypting with the receiver's public key provides confidentiality.**
B. Signing can only occur using the sender's private key.
C. The sender would not have access to the receiver's private key.
D. By encrypting the message with the receiver's public key, only the receiver can decrypt the message using their own private key. The receiver's private key is confidential and, therefore, unknown to the sender. Messages encrypted using the sender's private key can be read by anyone with the sender's public key.

A5-106 An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the **BEST** protection against hacking?

A. An application-level gateway
B. A remote access server
C. A proxy server
D. Port scanning

A is the correct answer.

Justification:

A. **An application-level gateway is the best way to protect against hacking because it can be configured with detailed rules that describe the type of user or connection that is or is not permitted. It analyzes, in detail, each package—not only in layers one through four of the Open System Interconnection model, but also layers five through seven, which means that it reviews the commands of each higher-level protocol (Hypertext Transmission Protocol, File Transfer Protocol, Simple Network Management Protocol, etc.).**
B. For a remote access server, there is a device (server) that asks for a username and password before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet, creating security exposure.
C. Proxy servers can provide excellent protection, but depending on the type of proxy, they may not be able to examine traffic as effectively as an application gateway. For proxy servers to work, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program.
D. Port scanning is used to detect vulnerabilities or open ports on a network, but not when trying to control what comes from the Internet, or when all the ports available need to be controlled. For example, the port for Ping (echo request) could be blocked and the IP addresses would be available for the application and browsing but would not respond to Ping.

A5-107 Which of the following is the **MOST** secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

A. Virtual private network
B. Dedicated line
C. Leased line
D. Integrated services digital network

A is the correct answer.

Justification:

A. The most secure method is a virtual private network, using encryption, authentication and tunneling to allow data to travel securely from a private network to the Internet.
B. A dedicated line is quite expensive and only needed when there are specific confidentiality and availability needs.
C. A leased line is an expensive but private option, but rarely a good option today.
D. Integrated services digital network is not encrypted and would need additional security to be a valid option.

A5-108 The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

A. connecting points are available in the facility to connect laptops to the network.
B. users take precautions to keep their passwords confidential.
C. terminals with password protection are located in insecure locations.
D. terminals are located within the facility in small clusters under the supervision of an administrator.

A is the correct answer.

Justification:

A. Any person with wrongful intentions can connect a laptop to the network. The insecure connecting points make unauthorized access possible if the individual has knowledge of a valid user ID and password. The other choices are controls for preventing unauthorized network access.
B. If system passwords are not readily available for intruders to use, they must guess, introducing an additional factor and requires time.
C. System passwords provide protection against unauthorized use of terminals located in insecure locations.
D. Supervision is a very effective control when used to monitor access to a small operating unit or production resources.

A5-109 Which of the following functions is performed by a virtual private network?

A. Hiding information from sniffers on the net
B. Enforcing security policies
C. Detecting misuse or mistakes
D. Regulating access

A is the correct answer.

Justification:

A. A virtual private network (VPN) hides information from sniffers on the Internet using tunneling. It works based on encapsulation and encryption of sensitive traffic.
B. A VPN does support security policies related to secure communications, but its primary purpose is to protect data in transit.
C. A VPN does not check the content of packets, so it cannot detect misuse or mistakes.
D. A VPN is not used to regulate access. A user may have to log in to use a VPN, but that is not the purpose of the VPN.

A5-110 Applying a digital signature to data traveling in a network provides:

A. confidentiality and integrity.
B. security and nonrepudiation.
C. integrity and nonrepudiation.
D. confidentiality and nonrepudiation.

C is the correct answer.

Justification:
A. A digital signature does not encrypt the message, so it cannot provide confidentiality.
B. A digital signature does not encrypt the message, so it cannot provide security.
C. **A digital signature is created by signing a hash of a message with the private key of the sender. This provides for the integrity (through the hash) and the proof of origin (nonrepudiation) of the message.**
D. A digital signature does not provide confidentiality.

A5-111 Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to-consumer transactions via the Internet?

A. Customers are widely dispersed geographically, but the certificate authorities (CAs) are not.
B. Customers can make their transactions from any computer or mobile device.
C. The CA has several data processing subcenters to administer certificates.
D. The organization is the owner of the CA.

D is the correct answer.

Justification:
A. It is common to use a single certificate authority (CA). They do not need to be geographically dispersed.
B. The use of public key infrastructure and certificates allows flexible secure communications from many devices.
C. The CA will often have redundancy and failover capabilities to alternate data centers.
D. **If the CA belongs to the same organization, this would pose a risk. The management of a CA must be based on trusted and secure procedures. If the organization has not set in place the controls to manage the registration, distribution and revocation of certificates this could lead to a compromise of the certificates and loss of trust.**

A5-112 Which of the following is the **MOST** reliable method to ensure identity of sender for messages transferred across Internet?

A. Digital signatures
B. Asymmetric cryptography
C. Digital certificates
D. Message authentication code

C is the correct answer.

Justification:
A. Digital signatures are used for both authentication and integrity, but the identity of the sender would still be confirmed by the digital certificate.
B. Asymmetric cryptography, such as public key infrastructure, appears to authenticate the sender but is vulnerable to a man-in-the-middle attack.
C. **Digital certificates are issued by a trusted third party. The message sender attaches the certificate and the recipient can verify authenticity with the certificate repository.**
D. Message authentication code is used for message integrity verification.

A5-113 Which of the following is the **BEST** way for an IS auditor to determine the effectiveness of a security awareness and training program?

A. Review the security training program.
B. Ask the security administrator.
C. Interview a sample of employees.
D. Review the security reminders to employees.

C is the correct answer.

Justification:
A. A security training program may be well designed, but the results of the program will be determined by employee awareness.
B. Asking the security administrator would not show the effectiveness of a security awareness and training program because such a program should target more than just the administrator.
C. **Interviewing a sample of employees is the best way to determine the effectiveness of a security awareness and training program because overall awareness must be determined, and effective security is dependent on people. Reviewing the security training program would not be the ultimate indicator of the effectiveness of the awareness training.**
D. Reviewing the security reminders to the employees is not the best way to find out the effectiveness of the training awareness because sending reminders may result in little actual awareness.

A5-114 A laptop computer belonging to a company database administrator (DBA) and containing a file of production database passwords has been stolen. What should the organization do **FIRST**?

A. Send a report to the IS audit department.
B. Change the name of the DBA account.
C. Suspend the DBA account.
D. Change the database password.

D is the correct answer.

Justification:
A. While the IS audit department should be notified, this should not be the first action.
B. Changing the database administrator (DBA) account name could impact production database servers and thus would not be a good idea.
C. Suspending the DBA account could impact the production database servers and may not be effective if there is more than one DBA account sharing the same database password. The thief may guess the account names of the other DBAs.
D. **The password should be changed immediately because there is no way to know whether it has been compromised.**

A5-115 If inadequate, which of the following would be the **MOST** likely contributor to a denial-of-service attack?

A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

A is the correct answer.

Justification:
A. **Improper router configuration and rules could lead to an exposure to denial-of-service (DoS) attacks.**
B. An inefficient design of the internal network may also lead to a DoS but this is not as high a risk as router misconfiguration errors.
C. Updates to router software has led to a DoS in the past, but this is a subset of router configuration and rules.
D. Audit testing and review techniques can cause a DoS if tests disable systems or applications, but this is not the most likely risk.

A5-116 The Secure Sockets Layer protocol ensures the confidentiality of a message by using:

A. symmetric encryption.
B. message authentication codes.
C. hash function.
D. digital signature certificates.

A is the correct answer.

Justification:
A. **Secure Sockets Layer (SSL) uses a symmetric key for message encryption.**
B. A message authentication code is used for ensuring data integrity.
C. Hash function is used for generating a message digest which can provide message integrity; it is not used for message encryption.
D. Digital signature certificates are used by SSL for server authentication.

A5-117 The **PRIMARY** goal of a web site certificate is:

A. authentication of the web site that will be surfed.
B. authentication of the user who surfs through that site.
C. preventing surfing of the web site by hackers.
D. the same purpose as that of a digital certificate.

A is the correct answer.

Justification:
A. **Authenticating the site to be surfed is the primary goal of a web certificate.**
B. Authentication of a user is achieved through passwords and not by a web site certificate.
C. The site certificate does not prevent hacking, nor does it authenticate a person.
D. Web site certificates may serve the same purpose as a digital certificate, but the goal of certificates is authentication.

A5-118 An IS auditor performing detailed network assessments and access control reviews should **FIRST**:

A. determine the points of entry into the network.
B. evaluate users' access authorization.
C. assess users' identification and authorization.
D. evaluate the domain-controlling server configuration.

A is the correct answer.

Justification:
A. **In performing detailed network assessments and access control reviews, an IS auditor should first determine the points of entry to the system and review the points of entry, accordingly, for appropriate controls.**
B. Evaluation of user access authorization is an implementation issue for appropriate controls for the points of entry.
C. Assessment of user identification and authorization are implementation issues for appropriate controls for the points of entry.
D. Evaluation of the domain-controlling server configuration is not the first area to be reviewed. It will be reviewed once the network entry points have been identified.

A5-119 The MOST serious challenge in the operation of an intrusion detection system is:

A. filtering false-positives alerts.
B. learning vendor-specific protocols.
C. updating detection signatures.
D. blocking eligible connections.

A is the correct answer.

Justification:

A. **Because of the configuration and the way intrusion detection system (IDS) technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents—false positives, the equivalent of a false alarm. An IS auditor needs to be aware of this and should check for implementation of related controls (such as IDS tuning) and incident handling procedures (such as the screening process) to know if an event is a security incident or a false positive.**
B. It might be necessary to learn vendor-specific protocols or commands for interacting with IDS, however most vendors provide relevant documentation and trainings which could be quickly mastered by qualified IT personnel.
C. It is necessary to regularly update detection signatures, however majority of modern IDSs systems has built-in modules providing automated and secure updates.
D. Blocking suspicious connections is a characteristic of Intrusion Prevention Systems, which are different type of network security systems.

AS5-120 An IS auditor performing an audit has determined that developers have been granted administrative access to the virtual machine management console to manage their own servers used for software development and testing. Which of the following choices would be of **MOST** concern for the IS auditor?

A. Developers have the ability to create or de-provision servers.
B. Developers could gain elevated access to production servers.
C. Developers can affect the performance of production servers with their applications.
D. Developers could install unapproved applications to any servers.

A is the correct answer.

Justification:

A. **Virtualization offers the ability to create or destroy virtual machines (VMs) through the administrative interface with administrative access. While a developer would be unlikely to de-provision a production server, the administrative console would grant him/her the ability to do this, which would be a significant risk.**
B. When properly configured, the administrative console of a virtual server host does not allow an individual to bypass the authentication of the guest operating system (OS) to access the server. In this case, while the developers could potentially start, stop or even de-provision a production VM, they could not gain elevated access to the OS of the guest through the administrative interface.
C. While there could be instances where a software development team might use resource-intensive applications that could cause performance issues for the virtual host, the greater risk would be the ability to de-provision VMs.
D. When properly configured, the administrative console of a virtual server host does not allow an individual to bypass the authentication of the guest OS to access the server; therefore, the concern that unauthorized software could be installed is not valid.

A5-121 Which of the following findings would be of **GREATEST** concern to an IS auditor during a review of logical access to an application?

A. Some developers have update access to production data.
B. The file storing the application ID password is in cleartext in the production code.
C. The change control team has knowledge of the application ID password.
D. The application does not enforce the use of strong passwords.

B is the correct answer.

Justification:
A. Developers might need limited update access to production data to perform their jobs and this access, when approved and reviewed by management, is acceptable even though it does pose a risk.
B. Compromise of the application ID password can result in untraceable, unauthorized changes to production data; storing the password in cleartext poses the greatest risk. While the production code may be protected from update access, it is viewable by development teams.
C. Knowledge of the application ID password by the change control team does not pose a great concern if adequate separation of duties exists between change control and development activities. There may be occasions when the application ID needs to be used by change control in the production environment.
D. While the lack of a strong password policy and configuration can result in compromised accounts, the risk is lower than if the application ID password is compromised because the application ID password does not allow for traceability.

A5-122 The management of an organization has decided to establish a security awareness program. Which of the following would **MOST** likely be a part of the program?

A. Using an intrusion detection system to report incidents
B. Mandating the use of passwords to access all software
C. Installing an efficient user log system to track the actions of each user
D. Training provided on a regular basis to all current and new employees

D is the correct answer.

Justification:
A. Using an intrusion detection system to report incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program.
B. Mandating the use of passwords is a policy decision, not an awareness issue.
C. Installing an efficient user log system is not a part of an awareness program.
D. Regular training is an important part of a security awareness program.

A5-123 A company determined that its web site was compromised, and a rootkit was installed on the server hosting the application. Which of the following choices would have **MOST** likely prevented the incident?

A. A host-based intrusion prevention system
B. A network-based intrusion detection system
C. A firewall
D. Operating system patching

A is the correct answer.

Justification:

A. **A host-based intrusion prevention system (IPS) prevents unauthorized changes to the host. If a malware attack attempted to install a rootkit, the IPS would refuse to permit the installation without the consent of an administrator.**
B. A network-based intrusion detection system (IDS) relies on attack signatures based on known exploits and attack patterns. If the IDS is not kept up to date with the latest signatures, or the attacker is able to create or gain access to an exploit unknown to the IDS, it will go undetected. A web server exploit performed through the web application itself, such as a Structured Query Language injection attack, would not appear to be an attack to the network-based IDS.
C. A firewall by itself does not protect a web server because the ports required for users to access the web server must be open in the firewall. Web server attacks are typically performed over the same ports that are open for normal web traffic. Therefore, a firewall does not protect the web server.
D. Operating system (OS) patching will make exploitation of the server more difficult for the attacker and less likely. However, attacks on the web application and server OS may succeed based on issues unrelated to any unpatched server vulnerabilities, and the host-based IPS should detect any attempts to change files on the server, regardless of how access was obtained.

A5-124 The role of the certificate authority (CA) as a third party is to:

A. provide secured communication and networking services based on certificates.
B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
C. act as a trusted intermediary between two communication partners.
D. confirm the identity of the entity owning a certificate issued by that CA.

D is the correct answer.

Justification:

A. Providing a communication infrastructure is not a certificate authority (CA) activity.
B. The secret keys belonging to the certificates would not be archived at the CA.
C. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.
D. **The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued.**

A5-125 Which of the following types of penetration tests effectively evaluates the incident handling and response capability of the system administrator?

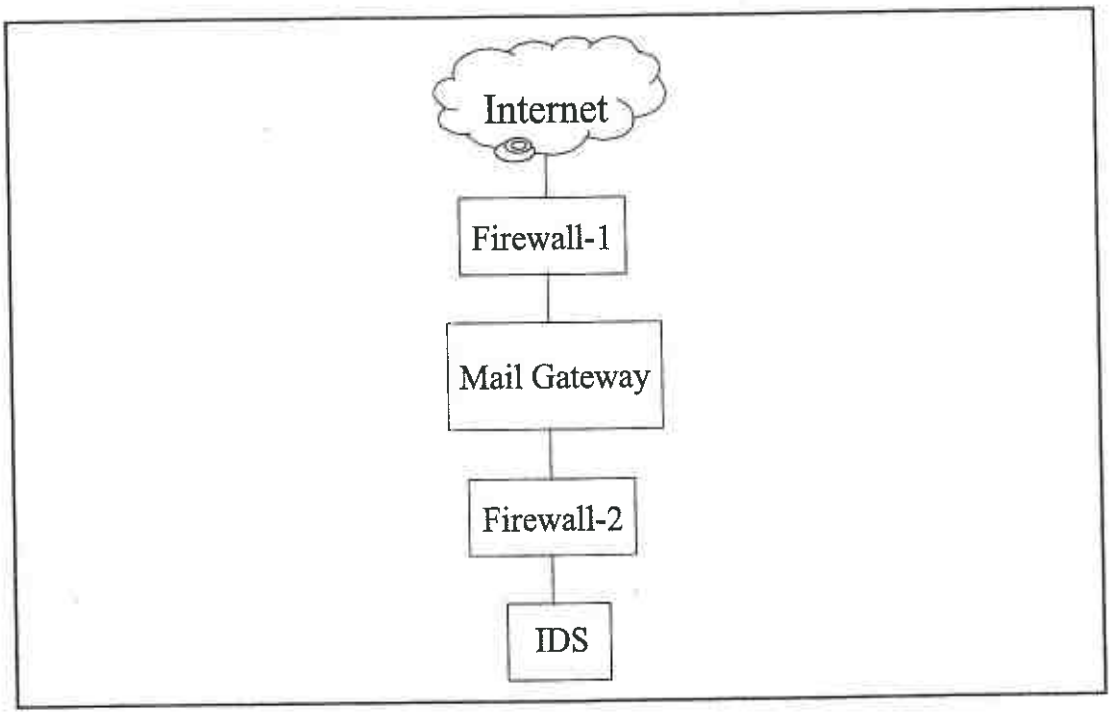
A. Targeted testing
B. Internal testing
C. Double-blind testing
D. External testing

C is the correct answer.

Justification:

A. In targeted testing, penetration testers are provided with information related to target and network design and the target's IT team is aware of the testing activities.
B. Internal testing refers to attacks and control circumvention attempts on the target from within the perimeter. The system administrator is typically aware of the testing activities.
C. **In double-blind testing, the penetration tester has little or limited knowledge about the target system, and personnel at the target site have not been informed that a test is being performed. Because the administrator and security staff at the target are not aware of the test, it can effectively evaluate the incident handling and response capability of the system administrator.**
D. External testing is a generic term that refers to attacks and control circumvention attempts on the target from outside the target system. The system administrator may or may not be aware of the testing activities, so this is not the correct answer. (Note: Rather than concentrating on specific terms, CISA candidates should understand the differences between various types of penetration testing.)

Question **A5-126** refers to the following diagram.



A5-126 Email traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network. The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The **FIRST** action triggered by the IDS should be to:

A. alert the appropriate staff.
B. create an entry in the log.
C. close firewall-2.
D. close firewall-1.

B is the correct answer.

Justification:

A. The first action taken by an intrusion detection system (IDS) will be to create a log entry and then alert the appropriate staff.
B. Creating an entry in the log is the first step taken by a network IDS. The IDS may also be configured to send an alert to the administrator, send a note to the firewall and may even be configured to record the suspicious packet.
C. Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been be caused by an attack from a hacker. After the IDS has logged the suspicious traffic, it may signal firewall-2 to close, thus preventing damage to the internal network. After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator, valuable time can be lost, in which a hacker could also compromise firewall-2.
D. The IDS will usually only protect the internal network by closing firewall-2 and will not close the externally facing firewall-1.

A5-127 An organization has experienced a large amount of traffic being re-routed from its Voice-over Internet Protocol packet network. The organization believes it is a victim of eavesdropping. Which of the following could result in eavesdropping of VoIP traffic?

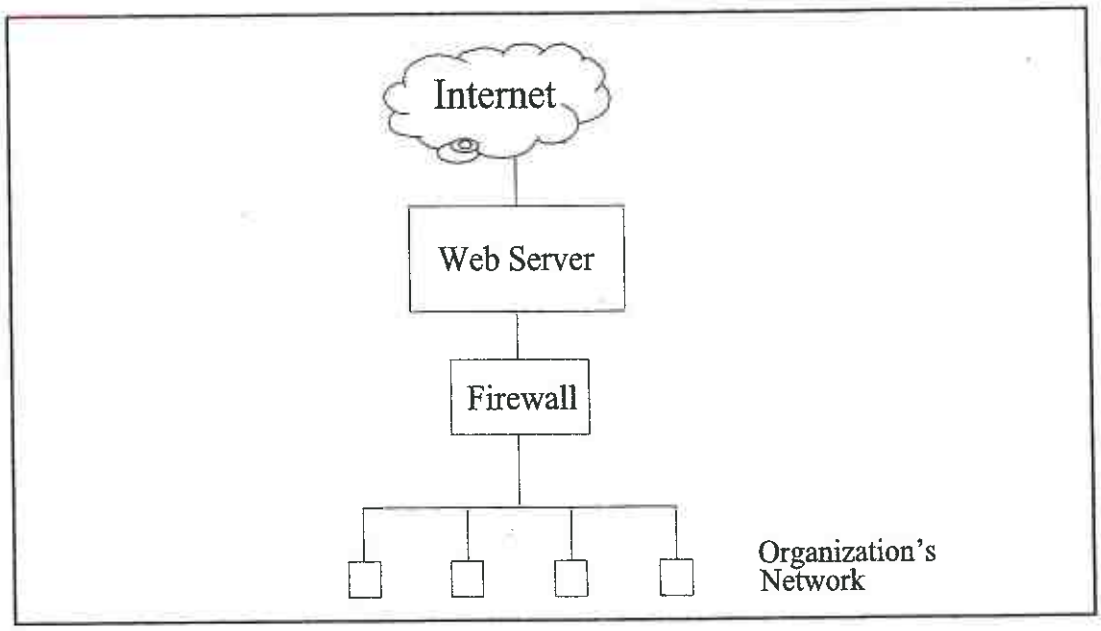
A. Corruption of the Address Resolution Protocol cache in Ethernet switches
B. Use of a default administrator password on the analog phone switch
C. Deploying virtual local area networks without enabling encryption
D. End users having access to software tools such as packet sniffer applications

A is the correct answer.

Justification:

A. On an Ethernet switch there is a data table known as the Address Resolution Protocol (ARP) cache, which stores mappings between media access control and IP addresses. During normal operations, Ethernet switches only allow directed traffic to flow between the ports involved in the conversation and no other ports can see that traffic. However, if the ARP cache is intentionally corrupted with an ARP poisoning attack, some Ethernet switches simply "flood" the directed traffic to all ports of the switch, which could allow an attacker to monitor traffic not normally visible to the port where the attacker was connected, and thereby eavesdrop on Voice-over Internet Protocol (VoIP) traffic.
B. VoIP systems do not use analog switches and inadequate administrator security controls would not be an issue.
C. VoIP data are not normally encrypted in a LAN environment because the controls regarding VLAN security are adequate.
D. Most software tools such as packet sniffers cannot make changes to LAN devices, such as the VLAN configuration of an Ethernet switch used for VoIP. Therefore, the use of software utilities of this type is not a risk.

Question **A5-128** refers to the following diagram.



A5-128 To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system between the:

A. Firewall and the organization's network.
B. Internet and the firewall.
C. Internet and the web server.
D. Web server and the firewall.

A is the correct answer.

Justification:

A. **Attack attempts that could not be recognized by the firewall will be detected if a network-based intrusion detection system (IDS) is placed between the firewall and the organization's network.**
B. A network-based IDS placed between the Internet and the firewall will detect attack attempts, whether they are or are not noticed by the firewall.
C. Placing an IDS outside of the web server will identify attacks directed at the web server but will not detect attacks missed by the firewall.
D. Placing the IDS after the web server would identify attacks that have made it past the web server but will not indicate whether the firewall would have been able to detect the attacks.

A5-129 An IS auditor is reviewing the physical security controls of a data center and notices several areas for concern. Which of the following areas is the **MOST** important?

A. The emergency power off button cover is missing.
B. Scheduled maintenance of the fire suppression system was not performed.
C. There are no security cameras inside the data center.
D. The emergency exit door is blocked.

D is the correct answer.

Justification:

A. The emergency power off button issue is a significant concern, but life safety is the highest priority.
B. The primary purpose of the fire suppression system is to protect the equipment and building. The lack of scheduled maintenance is a concern; however, this does not indicate that the system would not function as required. The more critical issue is the emergency exit because life safety is the highest priority.
C. The lack of security cameras inside the data center may be a significant concern; however, the more significant issue is the emergency exit door being blocked.
D. Life safety is always the highest priority; therefore, the blocking of the emergency exit is the most serious problem.

A5-130 Which of the following choices **BEST** helps information owners to properly classify data?

A. Understanding of technical controls that protect data
B. Training on organizational policies and standards
C. Use of an automated data leak prevention tool
D. Understanding which people need to access the data

B is the correct answer.

Justification:

A. While understanding how the data are protected is important, these controls might not be applied properly if the data classification schema is not well understood.
B. While implementing data classification, it is most essential that organizational policies and standards, including the data classification schema, are understood by the owner or custodian of the data so they can be properly classified.
C. While an automated data leak prevention (DLP) tool may enhance productivity, the users of the application would still need to understand what classification schema was in place.
D. In terms of protecting the data, the data requirements of end users are critical, but if the data owner does not understand what data classification schema is in place, it would be likely that inappropriate access to sensitive data might be granted by the data owner.

A5-131 While auditing an internally developed web-application, an IS auditor determines that all business users share a common access profile. Which of the following is the **MOST** relevant recommendation to prevent the risk on unauthorized data modification?

A. Enable detailed logging of user actions.
B. Customize user access profiles per job responsibility.
C. Enforce strong password policy for all accounts.
D. Implement regular access rights review.

B is the correct answer.

Justification:
A. Logging is a detective control and often a secondary recommendation in the event that technical issues or costs prohibit implementation of preventive controls.
B. The strongest control is a preventive control that is automated through the system. Developing additional access profiles would ensure that the system restricts users to privileges defined by their job responsibilities and that an audit trail exists for those user actions.
C. While a enforcing password policy is a type of preventive control, it is not as effective as removing excessive access rights from users who do not need it to perform their job duties.
D. Access right review will not help in this scenario, because all profiles have similar set of access rights.

A5-132 Which of the following is the **MOST** important security consideration to an organization that wants to move a business application to external cloud-service (PaaS) provided by a vendor?

A. Classification and categories of data process by the application.
B. Cost of hosting the application internally versus externally.
C. A reputation of a vendor on the market and feedbacks from clients.
D. Drop of application performance due to use of shared services.

A is the correct answer.

Justification:
A. Types of data and its sensitivity is a primary consideration, as there might be legal obligations related to data hosting and its level of protection (e.g. personal information, banking information, health information, etc.)
B. Cost is an important factor for an organization to consider during the move to cloud, however the highest risk is to violate data privacy laws.
C. A reputation of a vendor on the market is an important factor for an organization to consider during the move to cloud, however the highest risk is to violate data privacy laws.
D. Drop of application performance due to use of shared services is an important factor for an organization to consider during the move to cloud, however the highest risk is to violate data privacy laws.

A5-133 Which of the following is **BEST** suited for secure communications within a small group?

A. Key distribution center
B. Certificate authority
C. Web of trust
D. Kerberos Authentication System

C is the correct answer.

Justification:

A. A key distribution center is a part of a Kerberos implementation suitable for internal communication for a large group within an institution, and it will distribute symmetric keys for each session.
B. Certificate authority is a trusted third party that ensures the authenticity of the owner of the certificate. This is necessary for large groups and formal communication.
C. **Web of trust is a key distribution method suitable for communication in a small group. It is used by tools such as pretty good privacy and distributes the public keys of users within a group.**
D. A Kerberos Authentication System extends the function of a key distribution center by generating "tickets" to define the facilities on networked machines, which are accessible to each user.

A5-134 Which of the following is the **MOST** important action in recovering from a cyberattack?

A. Activating an incident response team
B. Hiring cyberforensic investigators
C. Executing a business continuity plan
D. Preserving evidence

A is the correct answer.

Justification:

A. **Hopefully the incident response team and procedures were set up prior to the cyberattack. The first step is to activate the team, contain the incident and keep the business operational.**
B. When a cyberattack is suspected, cyberforensic investigators should be used to set up alarms, catch intruders within the network, and track and trace them over the Internet. The use of cyberforensic experts is only done after the incident has been identified.
C. The most important objective in recovering from a cyberattack is to keep the business operational, but most attacks will not require the activation or use of the business continuity plan.
D. The primary objective for the business is to stay in business. In a noncriminal investigation this may even mean that some evidence is lost.

A5-135 What method might an IS auditor use to test wireless security at branch office locations?

A. War dialing
B. Social engineering
C. War driving
D. Password cracking

C is the correct answer.

Justification:

A. War dialing is a technique for gaining access to a computer or a network through the dialing of defined blocks of telephone numbers, with the hope of getting an answer from a modem.
B. Social engineering is a technique used to gather information that can assist an attacker in gaining logical or physical access to data or resources. Social engineering exploits human weaknesses.
C. **War driving is a technique for locating and gaining access to wireless networks by driving or walking around a building with a wireless-equipped computer.**
D. Password crackers are tools used to guess users' passwords by trying combinations and dictionary words. Once a wireless device has been identified, password crackers may be used to try to attack it.

A5-136 Which of the following intrusion detection systems will **MOST** likely generate false alarms resulting from normal network activity?

A. Statistical-based
B. Signature-based
C. Neural network
D. Host-based

A is the correct answer.

Justification:

A. **A statistical-based intrusion detection system (IDS) relies on a definition of known and expected behavior of systems. Because normal network activity may, at times, include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious.**
B. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. Signature-based systems traditionally have low levels of false positives but may be weak at detecting new attacks.
C. A neural network combines the statistical- and signature-based IDSs to create a hybrid and better system.
D. Host-based is another type of IDS, but it would not be used to monitor network activity.

A5-137 When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

A. hardware is protected against power surges.
B. integrity is maintained if the main power is interrupted.
C. immediate power will be available if the main power is lost.
D. hardware is protected against long-term power fluctuations.

A is the correct answer.

Justification:

A. **A voltage regulator protects against short-term power fluctuations.**
B. A voltage regulator does not maintain the integrity if power is interrupted or lost.
C. An uninterruptible power supply (UPS) is used to provide constant power even if main power is lost.
D. A voltage regulator protects against short-term power fluctuations.

A5-138 In an organization where an IT security baseline has been defined an IS auditor should **FIRST** ensure:

A. implementation.
B. compliance.
C. documentation.
D. sufficiency.

D is the correct answer.

Justification:

A. The first step is to review the baseline to ensure that it is adequate or sufficient to meet the security requirements of the organization. Then the IS auditor will ensure that it is implemented and measure compliance.
B. Compliance cannot be measured until the baseline has been implemented, but the IS auditor must first ensure that the correct baseline is being implemented.
C. After the baseline has been defined, it must be documented, and the IS auditor will check that the baseline is appropriate before checking for implementation.
D. **An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of the control baseline to meet security requirements.**

A5-139 Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

A. Power line conditioners
B. Surge protective devices
C. Alternative power supplies
D. Interruptible power supplies

A is the correct answer.

Justification:

A. **Power line conditioners are used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine. Any valleys are removed by power stored in the equipment.**
B. Surge protection devices protect against high-voltage bursts.
C. Alternative power supplies are intended for power failures that last for longer periods and are normally coupled with other devices such as an uninterruptible power supply to compensate for the power loss until the alternate power supply becomes available.
D. An interruptible power supply would cause the equipment to come down whenever there was a power failure.

A5-140 An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers—one filled with carbon dioxide (CO_2), the other filled with halon gas. Which of the following should be given the **HIGHEST** priority in the IS auditor's report?

A. The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
B. Both fire suppression systems present a risk of suffocation when used in a closed room.
C. The CO_2 extinguisher should be removed, because CO_2 is ineffective for suppressing fires involving solid combustibles (paper).
D. The documentation binders should be removed from the equipment room to reduce potential risk.

B is the correct answer.

Justification:

A. The Montreal Protocol allows existing halon installations to remain, although some countries may have laws that require its removal.
B. **Protecting people's lives should always be of highest priority in fire suppression activities. Carbon dioxide (CO_2) and halon both reduce the oxygen ratio in the atmosphere, which can induce serious personal hazards. In many countries, installing or refilling halon fire suppression systems is not allowed.**
C. CO_2 extinguishers can be used on most types of fires, and their use in a server room would be appropriate.
D. Although not of highest priority, removal of the documentation would probably reduce some of the risk.

A5-141 What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

A. Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
B. The contingency plan for the organization cannot effectively test controlled access practices.
C. Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
D. Removing access for those who are no longer authorized is complex.

A is the correct answer.

Justification:
A. **Piggybacking or tailgating can compromise the physical access controls.**
B. The testing of controlled access would be of minimal concern in a disaster recovery environment.
C. Duplicating access control cards or keys is technically challenging.
D. An access control system should have easily followed procedures for managing user access throughout the access life cycle.

A5-142 An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is **MOST** important?

A. False-acceptance rate
B. Equal-error rate
C. False-rejection rate
D. False-identification rate

A is the correct answer.

Justification:
A. **False-acceptance rate (FAR) is the frequency of accepting an unauthorized person as authorized, thereby granting access when it should be denied. In an organization with high security requirements, limiting the number of false acceptances is more important that the impact on the false reject rate.**
B. Equal-error rate (EER) (also called the crossover error rate) is the point where the FAR equals the false-rejection rate (FRR). This is the criteria used to measure the optimal accuracy of the biometric system, but in a highly secure environment, the FAR is more important that the EER.
C. FRR denies an authorized person access, but this is less important than the FAR because it is better to deny access to an authorized individual than to grant access to an unauthorized individual.
D. False-identification rate (FIR) is the probability that an authorized person is identified, but is assigned a false ID.

A5-143 Which of the following groups would create **MOST** concern to an IS auditor if they have full access to the production database?

A. Application developers
B. System administrators
C. Business users
D. Information security team

A is the correct answer.

Justification:

A. **Application developers having the access to production environment bear the highest risk. Due to their focus on delivery of changes, they tend to bypass quality assurance controls installing deficient changes into production environment.**
B. System administrators may require full production access to conduct their administration duties; however, they should be monitored for unauthorized activity.
C. Business users might not need a full access to database. Such set up might result in negatives scenarios (fraud), however developers having a direct access to production environment is a higher concern.
D. The data recovery team will need full access to make sure the complete database is recoverable.

A5-144 The **BEST** overall quantitative measure of the performance of biometric control devices is:

A. false-rejection rate.
B. false-acceptance rate.
C. equal-error rate.
D. estimated-error rate.

C is the correct answer.

Justification:

A. The false-rejection rate (FRR) only measures the number of times an authorized person is denied entry.
B. The false-acceptance rate (FAR) only measures the number of times an unauthorized person may be accepted as authorized.
C. **A low equal-error rate (EER) is a combination of a low FRR and a low FAR. EER, expressed as a percentage, is a measure of the number of times that the FRR and FAR are equal. A low EER is the measure of the more effective biometrics control device.**
D. The estimated-error rate is not a valid biometric term.

A5-145 Which of the following is the **MOST** effective control over visitor access to a data center?

A. Visitors are escorted.
B. Visitor badges are required.
C. Visitors sign in.
D. Visitors are spot-checked by operators.

A is the correct answer.

Justification:

A. **Escorting visitors will provide the best assurance that visitors have permission to access defined areas within the data processing facility.**
B. Requiring visitors to wear badges is a good practice, but not a reliable control.
C. Requiring that visitors sign in is good practice, but not a reliable control. After visitors are in the building, the sign-in process will not prevent them from accessing unauthorized areas.
D. Visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

A5-146 In a public key infrastructure, a registration authority:

A. verifies information supplied by the subject requesting a certificate.
B. issues the certificate after the required attributes are verified and the keys are generated.
C. digitally signs a message to achieve nonrepudiation of the signed message.
D. registers signed messages to protect them from future repudiation.

A is the correct answer.

Justification:

A. **A registration authority is responsible for verifying information supplied by the subject requesting a certificate and verifies the requestor's right to request a certificate on behalf of themselves or their organization.**
B. Certification authorities, not registration authorities, actually issue certificates once verification of the information has been completed.
C. The sender who has control of his/her private key signs the message, not the registration authority.
D. Registering signed messages is not a task performed by registration authorities.

A5-147 Confidentiality of the data transmitted in a wireless local area network is **BEST** protected if the session is:

A. restricted to predefined media access control addresses.
B. encrypted using static keys.
C. encrypted using dynamic keys.
D. initiated from devices that have encrypted storage.

C is the correct answer.

Justification:

A. Limiting the number of devices that can access the network via media access control address filtering is an inefficient control and does not address the issue of encrypting the session.
B. Encryption with static keys—using the same key for a long period of time—carries a risk that the key would be compromised.
C. **When using dynamic keys, the encryption key is changed frequently, thus reducing the risk of the key being compromised and the message being decrypted.**
D. Encryption of the data on the connected device (laptop, smart phone, etc.) addresses the confidentiality of the data on the device, not the wireless session.

A5-148 Which of the following provides the **MOST** relevant information for proactively strengthening security settings?

A. Bastion host
B. Intrusion detection system
C. Honeypot
D. Intrusion prevention system

C is the correct answer.

Justification:

A. A bastion host is a hardened system used to host services. It does not provide information about an attack.
B. Intrusion detection systems are designed to detect and address an attack in progress and stop it as soon as possible.
C. **The design of a honeypot is such that it lures the hacker and provides clues as to the hacker's methods and strategies, and the resources required to address such attacks. A honeypot allows the attack to continue, so as to obtain information about the hacker's strategy and methods.**
D. Intrusion prevention systems are designed to detect and address an attack in progress and stop it as soon as possible.

A5-149 Over the long term, which of the following has the greatest potential to improve the security incident response process?

A. A walk-through review of incident response procedures
B. Simulation exercises performed by incident response team
C. Ongoing security training for users
D. Documenting responses to an incident

B is the correct answer.

Justification:
A. A walk-through is a good first step to evaluate the incident response plan, but the lessons learned from incidents will provide more meaningful long-term benefits.
B. Simulation exercises to find the gaps and shortcomings in the actual incident response processes will help improve the process over time.
C. Training the users and members of the incident response team will improve the effectiveness of the team but learning from the lessons of previous incidents will generate the greatest benefit.
D. Documenting all incidents is important to allow later analysis and review but is not as important as the results of the analysis.

A5-150 When reviewing an intrusion detection system, an IS auditor should be **MOST** concerned about which of the following?

A. High number of false-positive alarms
B. Low coverage of network traffic
C. Network performance downgrade
D. Default detection settings

B is the correct answer.

Justification:
A. Although the number of false-positives is a serious issue, the problem will be known and can be corrected.
B. The cybersecurity attacks might not be timely identified if only small portion of network traffic is analyzed.
C. Intrusion detection system might decrease an overall network performance, however it is a secondary risk in this case.
D. It is a good practice to customize IDS settings to specific network perimeter, however there is a higher likelihood to miss the attacks due to insufficient network coverage.

A5-151 Distributed denial-of-service attacks on Internet sites are typically evoked by hackers using which of the following?

A. Logic bombs
B. Phishing site
C. Spyware
D. Botnets

D is the correct answer.

Justification:
A. Logic bombs are programs designed to destroy or modify data at a specific event or time in the future.
B. Phishing is an attack, normally via email, pretending to be an authorized person or organization requesting information.
C. Spyware is a program that picks up information from PC drives by making copies of their contents.
D. A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection.

A5-152 Validated digital signatures in an email software application will:

A. help detect spam.
B. provide confidentiality.
C. add to the workload of gateway servers.
D. significantly reduce available bandwidth.

A is the correct answer.

Justification:

A. **Validated electronic signatures are based on qualified certificates that are created by a certificate authority, with the technical standards required to ensure the key can neither be forced nor reproduced in a reasonable time. Such certificates are only delivered through a registration authority after a proof of identity has been passed. Using strong signatures in email traffic, nonrepudiation can be assured, and a sender can be tracked. The recipient can configure his/her email server or client to automatically delete emails from specific senders.**
B. For confidentiality issues, one must use encryption, not a signature.
C. Without any filters directly applied on mail gateway servers to block traffic without strong signatures, the workload will not increase. Using filters directly on a gateway server will result in an overhead less than antivirus software imposes.
D. Digital signatures are only a few bytes in size and will not slash bandwidth. Even if gateway servers were to check certificate revocation lists, there is little overhead.

A5-153 In transport mode, the use of the Encapsulating Security Payload protocol is advantageous over the authentication header protocol because it provides:

A. connectionless integrity.
B. data origin authentication.
C. antireplay service.
D. confidentiality.

D is the correct answer.

Justification:

A. Both forms of Internet Protocol security (IPSec), authentication header (AH) and encapsulating security payload (ESP), provide connectionless integrity.
B. Both AH and ESP authenticate data origin.
C. The time stamps used in IPSec will prevent replay attacks.
D. **Only the ESP protocol provides confidentiality via encryption.**

A5-154 IS management recently replaced its existing wired local area network with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

A. Port scanning
B. Back door
C. Man-in-the-middle
D. War driving

D is the correct answer.

Justification:

A. Port scanning will often target the external firewall of the organization. Use of wireless will not affect this.
B. A back door is an opening implanted into or left in software that enables an unauthorized entry into a system.
C. Man-in-the-middle attacks intercept a message and can read, replace or modify it.
D. A war driving attack uses a wireless Ethernet card, set in promiscuous mode, and a powerful antenna to penetrate wireless systems from outside.

A5-155 Which of the following is the **GREATEST** concern associated with the use of peer-to-peer computing?

A. Virus infection
B. Data leakage
C. Network performance issues
D. Unauthorized software usage

B is the correct answer.

Justification:

A. While peer-to-peer computing does increase the risk of virus infection, the risk of data leakage is more severe, especially if it contains proprietary data or intellectual property.
B. Peer-to-peer computing can share the contents of a user hard drive over the Internet. The risk that sensitive data could be shared with others is the greatest concern.
C. Peer-to-peer computing may use more network bandwidth and, therefore, may create performance issues. However, data leakage is a more severe risk.
D. Peer-to-peer computing may be used to download or share unauthorized software, which users could install on their PCs unless other controls prevent it. However, data leakage is a more severe risk.

A5-156 The IS management of a multinational company is considering upgrading its existing virtual private network to support Voice-over Internet Protocol communication via tunneling. Which of the following considerations should be **PRIMARILY** addressed?

A. Reliability and quality of service
B. Means of authentication
C. Privacy of voice transmissions
D. Confidentiality of data transmissions

A is the correct answer.

Justification:

A. **Reliability and quality of service (QoS) are the primary considerations to be addressed. Voice communications require consistent levels of service, which may be provided through QoS and class of service controls.**
B. The company currently has a virtual private network (VPN); authentication has been implemented by the VPN using tunneling.
C. Privacy of voice transmissions is provided by the VPN protocol.
D. The company currently has a VPN; confidentiality of both data and Voice-over Internet Protocol traffic has been implemented by the VPN using tunneling.

A5-157 Which of the following antispam filtering methods has the **LOWEST** possibility of false-positive alerts?

A. Rule-based
B. Check-sum based
C. Heuristic filtering
D. Statistic-based

B is the correct answer.

Justification:

A. Rule-based filtering will trigger false-positive alert each time a key word is met in the message.
B. **The advantage of this type of filtering is that it lets ordinary users help identify spam, and not just administrators, thus vastly increasing the pool of spam fighters. The disadvantage is that spammers can insert unique invisible gibberish—known as hashbusters—into the middle of each of their messages, thus making each message unique and having a different checksum. This leads to an arms race between the developers of the checksum software and the developers of the spam-generating software.**
C. A heuristic is a technique designed for solving a problem more quickly when classic methods are too slow, or for finding an approximate solution when classic methods fail to find any exact solution. This is achieved by trading optimality, completeness, accuracy, or precision for speed. In a way, it can be considered a shortcut.
D. Statistical filtering analyze frequency of each word within the message and then evaluating the message as a whole. Therefore, it can ignore a suspicious keyword if the entire message is within normal bounds, however prone to false-positive alerts.

A5-158 Which of the following public key infrastructure (PKI) elements describes procedure for disabling a compromised private key?

A. Certificate revocation list
B. Certification practice statement
C. Certificate policy
D. PKI disclosure statement

B is the correct answer.

Justification:

A. The certificate revocation list is a list of certificates that have been revoked before their scheduled expiration date.
B. The certification practice statement is the how-to document used in policy-based public key infrastructure (PKI).
C. The certificate policy sets the requirements that are subsequently implemented by the CPS.
D. The PKI disclosure statement covers critical items such as the warranties, limitations and obligations that legally bind each party.

A5-159 The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

A. Replay
B. Brute force
C. Cryptographic
D. Mimic

A is the correct answer.

Justification:

A. Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access.
B. A brute force attack involves feeding the biometric capture device numerous different biometric samples.
C. A cryptographic attack targets the algorithm or the encrypted data.
D. In a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user such as forging a signature or imitating a voice.

A5-160 An IS auditor is reviewing system access and discovers an excessive number of users with privileged access. The IS auditor discusses the situation with the system administrator, who states that some personnel in other departments need privileged access and management has approved the access. Which of the following would be the **BEST** course of action for the IS auditor?

A. Determine whether compensating controls are in place.
B. Document the issue in the audit report.
C. Recommend an update to the procedures.
D. Discuss the issue with senior management.

A is the correct answer.

Justification:

A. An excessive number of users with privileged access is not necessarily an issue if compensating controls are in place.
B. An IS auditor should gather additional information before presenting the situation in the report.
C. An update to procedures would not address a potential weakness in logical security and may not be feasible if individuals are required to have this access to perform their jobs.
D. The IS auditor should gather additional information before reporting the item to senior management.

A5-161 Two-factor authentication can be circumvented through which of the following attacks?

A. Denial-of-service
B. Man-in-the-middle
C. Key logging
D. Brute force

B is the correct answer.

Justification:

A. A denial-of-service attack does not have a relationship to authentication.
B. A man-in-the-middle attack is similar to piggybacking in that the attacker pretends to be the legitimate destination, and then merely retransmits whatever is sent by the authorized user along with additional transactions after authentication has been accepted. This is done in many instances of bank fraud.
C. Key logging could circumvent single-factor authentication but not two-factor authentication.
D. Brute force could circumvent single-factor authentication but not two-factor authentication.

A5-162 An organization can ensure that the recipients of emails from its employees can authenticate the identity of the sender by:

A. digitally signing all email messages.
B. encrypting all email messages.
C. compressing all email messages.
D. password protecting all email messages.

A is the correct answer.

Justification:

A. By digitally signing all email messages, the receiver will be able to validate the authenticity of the sender.
B. Encrypting all email messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender.
C. Compressing all email messages would reduce the size of the message but would not ensure authenticity.
D. Password protecting all email messages would ensure that only those who have the password would be able to open the message; however, it would not ensure authenticity of the sender.

SCENARIO

A scenario is a mini-case study that describes a situation or an organization and requires candidates to answer one or more questions based on the information provided. A scenario can focus on a specific domain or on several domains. The CISA exam will include scenarios.

QUESTIONS A5-163 THROUGH A5-164 REFER TO THE FOLLOWING INFORMATION:

Company XYZ has outsourced production support to service provider ABC located in another country. The ABC service provider personnel remotely connect to the corporate network of the XYZ outsourcing entity over the Internet.

A5-163 Which of the following would provide the **BEST** assurance that only authorized users of ABC connect over the Internet for production support to XYZ?

A. Single sign-on authentication
B. Password complexity requirements
C. Two-factor authentication
D. Internet Protocol address restrictions

C is the correct answer.

Justification:

A. Single sign-on authentication provides a single access point to system resources. It would not be best in this situation.
B. While password complexity requirements would help prevent unauthorized access, two-factor authentication is a more effective control for this scenario.
C. Two-factor authentication is the best method to provide a secure connection because it uses two factors, typically "what you have" (for example, a device to generate one-time-passwords), "what you are" (for example, biometric characteristics) or "what you know" (for example, a personal identification number or password). Using a password in and of itself without the use of one or more of the other factors mentioned is not the best for this scenario.
D. Internet Protocol addresses can always change or be spoofed and, therefore, are not the best form of authentication for the scenario mentioned.

SEE INFORMATION PRECEDING QUESTION A5-163

A5-164 Which of the following would **BEST** provide assurance that transmission of information is secure while the production support team at ABC is providing support to XYZ?

A. Secret key encryption
B. Dynamic Internet Protocol address and port
C. Hash functions
D. Virtual private network tunnel

D is the correct answer.

Justification:

A. Secret key encryption would require sharing of the same key at the source and destination and involve an additional step for encrypting and decrypting data at each end. This is not a feasible solution given the scenario.
B. Using a dynamic Internet Protocol address and port is not an effective control because an attacker could easily find the new address using the domain name system.
C. While the use of a cryptographic hash function may be helpful to validate the integrity of data files, in this case it would not be useful for a production support team connecting remotely.
D. As ABC and XYZ are communicating over the Internet, which is an untrusted network, establishing an encrypted virtual private network tunnel would best ensure that the transmission of information was secure.

A5-165 The **PRIMARY** purpose of installing data leak prevention software is to:

A. restrict user access to confidential files stored on servers.
B. detect attempts to destroy sensitive data in an internal network.
C. block external systems from accessing internal resources.
D. control confidential documents leaving the internal network.

D is the correct answer.

Justification:

A. Access privileges to confidential files stored on the server will be controlled through digital rights management (DRM) software.
B. Potential attacks to systems on the internal network would normally be controlled through an intrusion detection system (IDS) and intrusion prevention system (IPS) as well as by security controls of the systems themselves. Data leak prevention (DLP) systems focus on data leaving the enterprise.
C. Controlling what external systems can access internal resources is the function of a firewall rather than a DLP system.
D. A server running a DLP software application uses predefined criteria to check whether any confidential documents or data are leaving the internal network.

A5-166 Which of the following is a control that can be implemented to reduce risk of internal fraud if application programmers are allowed to move programs into the production environment in a small organization?

A. Post-implementation functional testing
B. Registration and review of changes
C. Validation of user requirements
D. User acceptance testing

B is the correct answer.

Justification:

A. Independent postimplementation testing would not be as effective because the system could be accepted by the end user without detecting the undocumented functionality.
B. An independent review of the changes to the program in production could identify potential unauthorized changes, versions or functionality that the programmer had put into production.
C. An independent review of user requirements would not be as effective because the system could meet user requirements and still include undocumented functionalities.
D. An independent review of user acceptance would not be as effective because the system could be accepted by the end users, and the undocumented functionalities could remain undetected.

A5-167 A characteristic of User Datagram Protocol in network communications is:

A. packets may arrive out of order.
B. increased communication latency.
C. incompatibility with packet broadcast.
D. error correction may slow down processing.

A is the correct answer.

Justification:

A. User Datagram Protocol (UDP) uses a simple transmission model without implicit handshaking routines for providing reliability, ordering or data integrity. Thus, UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated or get dropped.
B. The advantage of UDP is that the lack of error checking allows for reduced latency. Time-sensitive applications, such as online video or audio, often use UDP because of the reduced latency of this protocol.
C. UDP is compatible with packet broadcast (sending to all on the local network) and multicasting (sending to all subscribers).
D. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.

A5-168 Which of the following choices is the **MOST** effective control that should be implemented to ensure accountability for application users accessing sensitive data in the human resource management system (HRMS) and among interfacing applications to the HRMS?

A. Two-factor authentication
B. A digital certificate
C. Audit trails
D. Single sign-on authentication

C is the correct answer.

Justification:

A. Two-factor authentication would enhance security while logging into the human resource management system application; however, it will not establish accountability for actions taken subsequent to login.
B. A digital certificate will also enhance login security to conclusively authenticate users logging into the application. However, it will not establish accountability because user ID and transaction details will not be captured without an audit trail.
C. **Audit trails capture which user, at what time, and date, along with other details, has performed the transaction and this helps in establishing accountability among application users.**
D. Single sign-on authentication allows users to log in seamlessly to the application, thus easing the authentication process. However, this would also not establish accountability.

A5-169 An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

A. reduces the risk of unauthorized access to the network.
B. is not suitable for small networks.
C. automatically provides an IP address to anyone.
D. increases the risk associated with Wireless Encryption Protocol (WEP).

A is the correct answer.

Justification:

A. **Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to anyone connecting to the network. With DHCP disabled, static IP addresses must be used, and this requires either administrator support or a higher level of technical skill to attach to the network and gain Internet access.**
B. DHCP is suitable for networks of all sizes from home networks to large complex organizations.
C. DHCP does not provide IP addresses when disabled.
D. Disabling of the DHCP makes it more difficult to exploit the well-known weaknesses in Wireless Encryption Protocol.

A5-170 Which of the following is **MOST** indicative of the effectiveness of an information security awareness program?

A. Employees report more information regarding security incidents.
B. All employees have signed the information security policy.
C. Most employees have attended an awareness session.
D. Information security responsibilities have been included in job descriptions.

A is the correct answer.

Justification:

A. **Although the promotion of security awareness is a preventive control, it can also be a detective measure because it encourages people to identify and report possible security violations. The reporting of incidents implies that employees are acting as a consequence of the awareness program.**
B. The existence of evidence that all employees have signed the security policy does not ensure that security responsibilities have been understood and applied.
C. One of the objectives of the security awareness program is to inform the employees of what is expected of them and what their responsibilities are, but this knowledge does not ensure that employees will perform their activities in a secure manner.
D. The documentation of roles and responsibilities in job descriptions is not an indicator of the effectiveness of the awareness program.

A5-171 An organization stores and transmits sensitive customer information within a secure wired network. It has implemented an additional wireless local area network (WLAN) to support general-purpose staff computing needs. A few employees with WLAN access have legitimate business reasons for also accessing customer information. Which of the following represents the **BEST** control to ensure separation of the two networks?

A. Establish two physically separate networks.
B. Implement virtual local area network segmentation.
C. Install a dedicated router between the two networks.
D. Install a firewall between the networks.

D is the correct answer.

Justification:

A. While having two physically separate networks would ensure the security of customer data, it would make it impossible for authorized wireless users to access that data.
B. While a VLAN would provide separation of the two networks, it is possible, with sufficient knowledge, for an attacker to gain access to one VLAN from the other.
C. A dedicated router between the two networks would separate them; however, this would be less secure than a firewall.
D. **In this case, a firewall could be used as a strong control to allow authorized users on the wireless network to access the wired network.**

A5-172 From a control perspective, the **PRIMARY** objective of classifying information assets is to:

A. establish guidelines for the level of access controls that should be assigned.
B. ensure access controls are assigned to all information assets.
C. assist management and auditors in risk assessment.
D. identify which assets need to be insured against losses.

A is the correct answer.

Justification:

A. **Information has varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources, management can establish guidelines for the level of access controls that should be assigned. End user management and the security administrator will use these classifications in their risk assessment process to assign a given class to each asset.**
B. Not all information needs to be protected through access controls. Overprotecting data would be expensive.
C. The classification of information is usually based on the risk assessment, not the other way around.
D. Insuring assets is valid; however, this is not the primary objective of information classification.

A5-173 An IS auditor reviewing access controls for a client-server environment should **FIRST**:

A. evaluate the encryption technique.
B. identify the network access points.
C. review the identity management system.
D. review the application level access controls.

B is the correct answer.

Justification:

A. Evaluating encryption techniques would be performed at a later stage of the review.
B. **A client-server environment typically contains several access points and uses distributed techniques, increasing the risk of unauthorized access to data and processing. To evaluate the security of the client server environment, all network access points should be identified.**
C. Reviewing the identity management system would be performed at a later stage of the review.
D. Reviewing the application level access controls would be performed at a later stage of the review.

A5-174 To prevent Internet Protocol (IP) spoofing attacks, a firewall should be configured to drop a packet for which the sender of a packet:

A. specifies the route that a packet should take through the network (the source routing field is enabled).
B. puts multiple destination hosts (the destination field has a broadcast address).
C. indicates that the computer should immediately stop using the TCP connection (a reset flag is turned on).
D. allows use of dynamic routing instead of static routing (Open Shortest Path First protocol is enabled).

A is the correct answer.

Justification:

A. **Internet Protocol (IP) spoofing takes advantage of the source-routing option in the IP. With this option enabled, an attacker can insert a spoofed source IP address. The packet will travel the network according to the information within the source-routing field, bypassing the logic in each router, including dynamic and static routing.**
B. If a packet has a broadcast destination address, it is definitely suspicious and if allowed to pass will be sent to all addresses in the subnet. This is not related to IP spoofing.
C. Turning on the reset flag is part of the normal procedure to end a Transmission Control Protocol connection.
D. The use of dynamic or static routing will not represent a spoofing attack.

A5-175 An IS auditor is reviewing a manufacturing company and finds that mainframe users at a remote site connect to the mainframe at headquarters over the Internet via Telnet. Which of the following offers the **STRONGEST** security?

A. Use of a point-to-point leased line
B. Use of a firewall rule to allow only the Internet Protocol address of the remote site
C. Use of two-factor authentication
D. Use of a nonstandard port for Telnet

A is the correct answer.

Justification:

A. **A leased line will effectively extend the local area network of the headquarters to the remote site, and the mainframe Telnet connection would travel over the private line, which would be less of a security risk when using an insecure protocol such as Telnet.**
B. A firewall rule at the headquarters network to only allow Telnet connections from the Internet Protocol (IP) address assigned to the remote site would make the connection more secure than the current arrangement, but a dedicated leased line is the most secure option of those listed.
C. While two-factor authentication would enhance the login security, it would not secure the transmission channel against eavesdropping, and, therefore, a leased line would be a better option.
D. Attacks on network services start with the assumption that network services use the standard Transmission Control Protocol/IP port number assigned for the service, which is port 23 for Telnet. By reconfiguring the host and client, a different port can be used. Assigning a nonstandard port for services is a good general security practice because it makes it more difficult to determine what service is using the port; however, in this case, creating a leased-line connection to the remote site would be a better solution.

A5-176 There is a concern that the risk of unauthorized access may increase after implementing a single sign-on process. To prevent unauthorized access, the **MOST** important action is to:

A. monitor failed authentication attempts.
B. review log files regularly.
C. deactivate unused accounts promptly.
D. mandate a strong password policy.

D is the correct answer.

Justification:

A. Ensuring that all failed authentication attempts are monitored is a good practice but is not a preventive control.
B. Reviewing the log files can increase the probability of detecting unauthorized access but will not prevent unauthorized access.
C. Ensuring that all unused accounts are deactivated is important; however, unauthorized access may occur via a regularly used account.
D. **Strong passwords are important in any environment but take on special importance in an SSO environment, where a user enters a password only one time and thereafter has general access throughout the environment. Of the options given, only a strong password policy offers broad preventative effects.**

A5-177 An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be **MOST** concerned if:

A. IDS sensors are placed outside of the firewall.
B. a behavior-based IDS is causing many false alarms.
C. a signature-based IDS is weak against new types of attacks.
D. the IDS is used to detect encrypted traffic.

B is the correct answer.

Justification:
A. An organization can place sensors outside of the firewall to detect attacks. These sensors are placed in highly sensitive areas and on extranets.
B. An excessive number of false alarms from a behavior-based intrusion detection system (IDS) indicates that additional tuning is needed. False positives cannot be eliminated entirely, but ignoring this warning sign may negate the value of the system by causing those responsible for monitoring its warnings to become convinced that anything reported is false.
C. Being weak against new types of attacks is expected from a signature-based IDS because it can only recognize attacks that have been previously identified.
D. An IDS cannot detect attacks within encrypted traffic, but there may be good reason to detect the presence of encrypted traffic, such as when a next-generation firewall is configured to terminate encrypted connections at the perimeter. In such cases, detecting encrypted packets flowing past the firewall could indicate improper configuration or even a compromise of the firewall itself.

A5-178 Which of the following **BEST** describes the role of a directory server in a public key infrastructure?

A. Encrypts the information transmitted over the network
B. Makes other users' certificates available to applications
C. Facilitates the implementation of a password policy
D. Stores certificate revocation lists

B is the correct answer.

Justification:
A. Encrypting the information transmitted over the network is a role performed by a security server.
B. A directory server makes other users' certificates available to applications.
C. Facilitating the implementation of a password policy is not relevant to public key infrastructure .
D. Storing certificate revocation lists is a role performed by a security server.

A5-179 An IS auditor is reviewing an organization's network operations center (NOC). Which of the following choices is of the **GREATEST** concern? The use of:

A. a wet pipe-based fire suppression system.
B. a rented rack space in the NOC.
C. a carbon dioxide-based fire suppression system.
D. an uninterrupted power supply with 10 minutes of backup power.

C is the correct answer.

Justification:
A. Wet pipe systems may damage computer equipment, but they are safe for humans and not as damaging as carbon dioxide (CO2) systems.
B. Rented rack space is not a concern as long as security controls are maintained. Most organizations rent server rack space.
C. CO2 systems should not be used in areas where people are present, because their function will cause suffocation in the event of a fire. Controls should consider personnel safety first.
D. Depending on the system, a few minutes might be all that is needed for a graceful shutdown. However, a CO2 system is dangerous for personnel.

A5-180 Inadequate programming and coding practices increase the risk of:

A. social engineering.
B. buffer overflow exploitation.
C. synchronize flood.
D. brute force attacks.

B is the correct answer.

Justification:

A. Social engineering attempts to gather sensitive information from people and primarily relies on human behavior. This is not a programming or coding problem.
B. Buffer overflow exploitation may occur when programs do not check the length of the data that are input into a program. An attacker can send data that exceed the length of a buffer and overwrite part of the program with arbitrary code, which will then be executed with the privileges of the program. The countermeasure is proper programming and good coding practices.
C. A synchronize (SYN) flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target system. A SYN flood is not related to programming and coding practices.
D. Brute force attacks are used against passwords and are not related to programming and coding practices.

A5-181 During an access control review for a mainframe application, an IS auditor discovers user security groups without designated owners. The **PRIMARY** reason that this is a concern to the IS auditor is that, without ownership, there is no one with clear responsibility for:

A. updating group metadata.
B. reviewing existing user access.
C. approval of user access.
D. removing terminated users.

C is the correct answer.

Justification:

A. Updating data about the group is not a great concern when compared to unauthorized access.
B. While the periodic review of user accounts is a good practice, this is a detective control and not as robust as preventing unauthorized access to the group in the first place.
C. Without an owner to provide approval for user access to the group, unauthorized individuals could potentially gain access to any sensitive data within the rights of the group.
D. Revoking access to terminated users is a compensating control for the normal termination process and is also a detective control.

A5-182 An IS auditor discovers that uniform resource locators (URLs) for online control self-assessment questionnaires are sent using URL shortening services. The use of URL shortening services would **MOST** likely increase the risk of which of the following attacks?

A. Spoofing
B. Phishing
C. Buffer overflow
D. Denial of service

B is the correct answer.

Justification:
A. Spoofing applies to source addressing, while uniform resource locator (URL) shortening applies to destination addressing.
B. URL shortening services have been adopted by hackers to fool users and spread malware (i.e., phishing)
C. Buffer overflows are not generally associated with URL shortening.
D. Denial-of-service attacks are not affected by URL shortening services.

A5-183 When installing an intrusion detection system, which of the following is **MOST** important?

A. Properly locating it in the network architecture
B. Preventing denial-of-service attacks
C. Identifying messages that need to be quarantined
D. Minimizing the rejection errors

A is the correct answer.

Justification:
A. Proper location of an intrusion detection system (IDS) in the network is the most important decision during installation. A poorly located IDS could leave key areas of the network unprotected.
B. A network IDS will monitor network traffic and a host-based IDS will monitor activity on the host, but it has no capability of preventing a denial-of-service (DoS) attack.
C. Configuring an IDS can be a challenge because it may require the IDS to "learn" what normal activity is, but the most important part of the installation is to install it in the right places.
D. An IDS is only a monitoring device and does not reject traffic. Rejection errors would apply to a biometric device.

A5-184 Which of the following is the **BEST** criterion for evaluating the adequacy of an organization's security awareness program?

A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.
B. Job descriptions contain clear statements of accountability for information security.
C. In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
D. No actual incidents have occurred that have caused a loss or a public embarrassment.

B is the correct answer.

Justification:

A. Senior management's level of awareness and concern for information assets is a criterion for evaluating the importance that they attach to those assets and their protection, but it is not as meaningful as having job descriptions that require all staff to be responsible for information security.
B. The inclusion of security responsibilities in job descriptions is a key factor in demonstrating the maturity of the security program and helps ensure that staff and management are aware of their roles with respect to information security.
C. Funding is important but having funding does not ensure that the security program is effective or adequate.
D. The number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program, but it is not a criterion for evaluating a security program.

A5-185 Which of the following features of a public key infrastructure is **MOST** closely associated with proving that an online transaction was authorized by a specific customer?

A. Nonrepudiation
B. Encryption
C. Authentication
D. Integrity

A is the correct answer.

Justification:

A. Nonrepudiation, achieved through the use of digital signatures, prevents the senders from later denying that they generated and sent the message.
B. Encryption plays a role in creating digital signatures, which are used to provide nonrepudiation, but encryption is also used for other purposes, whereas nonrepudiation is entirely concerned with ensuring that specific actions can be traced to specific actors in a manner beyond reasonable doubt.
C. Authentication is necessary to establish the identification of all parties to a communication but does not play a central role in the scenario described.
D. Integrity ensures that transactions are accurate but does not provide the identification of the customer.

A5-186 After reviewing its business processes, a large organization is deploying a new web application based on a Voice-over Internet Protocol technology. Which of the following is the **MOST** appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control
B. Role-based access control
C. Access control lists
D. Network/service access control

B is the correct answer.

Justification:

A. Fine-grained access control on Voice-over Internet Protocol (VoIP) web applications does not scale to enterprisewide systems because it is primarily based on individual user identities and their specific technical privileges.
B. Authorization in this case can best be addressed by role-based access control (RBAC) technology. RBAC controls access according to job roles or functions. RBAC is easy to manage and can enforce strong and efficient access controls in large-scale web environments including VoIP implementation.
C. Access control lists on VoIP web applications do not scale to enterprisewide systems because they are primarily based on individual user identities and their specific technical privileges.
D. Network/service addresses VoIP availability but does not address application-level access or authorization.

A5-187 During a logical access controls review, an IS auditor observes that user accounts are shared. The **GREATEST** risk resulting from this situation is that:

A. an unauthorized user may use the ID to gain access.
B. user access management is time consuming.
C. user accountability is not established.
D. passwords are easily guessed.

C is the correct answer.

Justification:

A. The risk of an unauthorized user accessing the system with a shared ID is no greater than an unauthorized user accessing the system with a unique user ID.
B. Access management would not be any different with shared IDs.
C. The use of a single user ID by more than one individual precludes knowing who, in fact, used that ID to access a system; therefore, it is more difficult to hold anyone accountable.
D. Shared user IDs do not necessarily have easily guessed passwords.

A5-188 To protect a Voice-over Internet Protocol infrastructure against a denial-of-service attack, it is **MOST** important to secure the:

A. access control servers.
B. session border controllers.
C. backbone gateways.
D. intrusion detection system.

B is the correct answer.

Justification:

A. Securing the access control server may prevent account alteration or lockout but is not the primary protection against denial-of-service (DoS) attacks.
B. Session border controllers enhance the security in the access network and in the core. In the access network, they hide a user's real address and provide a managed public address. This public address can be monitored, minimizing the opportunities for scanning and DoS attacks. Session border controllers permit access to clients behind firewalls while maintaining the firewall's effectiveness. In the core, session border controllers protect the users and the network. They hide network topology and users' real addresses. They can also monitor bandwidth and quality of service.
C. Backbone gateways are isolated and not readily accessible to hackers, so this is not a location of DoS attacks.
D. Intrusion detection systems monitor traffic, but do not protect against DoS attacks.

A5-189 In an online banking application, which of the following would **BEST** protect against identity theft?

A. Encryption of personal password
B. Restricting the user to a specific terminal
C. Two-factor authentication
D. Periodic review of access logs

C is the correct answer.

Justification:

A. A password alone is only single-factor authentication and could be guessed or broken.
B. Restricting the user to a specific terminal is not a practical alternative for an online application because the users may need to log in from multiple devices.
C. Two-factor authentication requires two independent methods for establishing identity and privileges. Factors include something you know such as a password; something you have such as a token; and something you are which is biometric. Requiring two of these factors makes identity theft more difficult.
D. Periodic review of access logs is a detective control and does not protect against identity theft.

A5-190 An IS auditor has found that employees are emailing sensitive company information to public web-based email domains. Which of the following is the **BEST** remediation option for the IS auditor to recommend?

A. Encrypted mail accounts
B. Training and awareness
C. Activity monitoring
D. Data loss prevention

D is the correct answer.

Justification:
A. Encrypted email accounts will secure the information being sent but will not prevent an employee from sending the information to an unauthorized person.
B. Training and awareness may influence employee behavior but are not effective as preventative controls when dealing with intentional exfiltration.
C. Activity monitoring is a detective control and will not prevent data from leaving the network.
D. Data loss prevention is an automated preventive tool that can block sensitive information from leaving the network, while at the same time logging the offenders. This is a better choice than relying on training and awareness because it works equally well when there is intent to steal data.

A5-191 Which of the following potentially blocks hacking attempts?

A. Intrusion detection system
B. Honeypot system
C. Intrusion prevention system
D. Network security scanner

C is the correct answer.

Justification:
A. An intrusion detection system is a detective control.
B. A honeypot solution captures intruder activity or traps the intruders when they attempt to explore a simulated target.
C. An intrusion prevention system is deployed as an inline device on a network or host that can detect and block hacking attempts.
D. A network security scanner identifies vulnerabilities but does not remediate them.

A5-192 A web server is attacked and compromised. Organizational policy states that incident response should balance containment of an attack with retaining freedom for later legal action against an attacker. Under the circumstances, which of the following should be performed **FIRST**?

A. Dump the volatile storage data to a disk.
B. Run the server in a fail-safe mode.
C. Disconnect the web server from the network.
D. Shut down the web server.

C is the correct answer.

Justification:
A. Dumping the volatile storage data to a disk may be used at the investigation stage but does not contain an attack in progress.
B. To run the server in a fail-safe mode, the server needs to be shut down.
C. **The first action is to disconnect the web server from the network to secure the device for investigation, contain the damage and prevent more actions by the attacker.**
D. Shutting down the server could potentially erase information that might be needed for a forensic investigation or to develop a strategy to prevent future similar attacks.

A5-193 What is the **BEST** approach to mitigate the risk of a phishing attack?

A. Intrusion detection
B. Security assessment
C. Strong authentication
D. User education

D is the correct answer.

Justification:

A. Intrusion detection systems (IDSs) will capture network or host traffic for analysis and may detect malicious activity but are not generally effective against phishing attacks.
B. Assessing security does not mitigate the risk. Phishing is based on social engineering and often distributed through email.
C. Phishing attacks can be mounted in various ways, often through email; strong two-factor authentication cannot mitigate most types of phishing attacks.
D. The best way to mitigate the risk of phishing is to educate users to take caution with suspicious Internet communications and not to trust them until verified. Users may require regular training to recognize suspicious web pages and email as the means and methods of threat actors evolve.

A5-194 A key IT systems developer has suddenly resigned from an enterprise. Which of the following will be the **MOST** important action?

A. Set up an exit interview with human resources.
B. Initiate the handover process to ensure continuity of the project.
C. Terminate the developer's logical access to IT resources.
D. Ensure that management signs off on the termination paperwork.

C is the correct answer.

Justification:

A. The interview with human resources (HR) is also an important process if it is conducted by the last date of employment, but it is of secondary importance compared to removing the developer's access to systems.
B. As long as the handover process to a designated employee is conducted by the last date of employment, there should be no problems.
C. To protect IT assets, terminating logical access to IT resources is the first and most important action to take after management has confirmed the employee's clear intention to leave the enterprise.
D. Ensuring that management signs off on termination paperwork is important, but not as critical as terminating access to the IT systems.

A5-195 Which of the following is a passive attack to a network?

A. Message modification
B. Masquerading
C. Denial-of-service
D. Traffic analysis

D is the correct answer.

Justification:

A. Message modification involves the capturing of a message and making unauthorized changes or deletions, changing the sequence or delaying transmission of captured messages. An attack that modifies the data would be an active attack.
B. Masquerading is an active attack in which the intruder presents an identity other than the original identity.
C. Denial-of-service occurs when a computer connected to the Internet is flooded with data and/or requests that must be processed. This is an active attack.
D. Traffic analysis allows a watching threat actor to determine the nature of the flow of traffic between defined hosts, which may allow the threat actor to guess the type of communication taking place without taking an active role.

A5-196 The **MOST** likely explanation for a successful social engineering attack is:

A. computer error.
B. judgment error.
C. expertise.
D. technology.

B is the correct answer.

Justification:

A. Social engineering focuses on human behavior.
B. Social engineering is fundamentally about obtaining from someone a level of trust that is not warranted.
C. Generally, social engineering attacks do not require significant expertise; often, the attacker is not proficient in information technology or systems.
D. Technology may facilitate social engineering, but it is fundamentally about obtaining human trust.

A5-197 A company is planning to install a network-based intrusion detection system to protect the web site that it hosts. Where should the device be installed?

A. On the local network
B. Outside the firewall
C. In the demilitarized zone
D. On the server that hosts the web site

C is the correct answer.

Justification:

A. While an intrusion detection system (IDS) can be installed on the local network to ensure that systems are not subject to internal attacks, a company's public web server would not normally be installed on the local network, but rather in the demilitarized zone (DMZ).
B. It is not unusual to place a network IDS outside of the firewall just to watch the traffic that is reaching the firewall, but this would not be used to specifically protect the web application.
C. **Network-based IDSs detect attack attempts by monitoring network traffic. A public web server is typically placed on the protected network segment known as the demilitarized zone (DMZ). An IDS installed in the DMZ detects and reports on malicious activity originating from the Internet as well as the internal network, thus allowing the administrator to act.**
D. A host-based IDS would be installed on the web server, but a network-based IDS would not.

A5-198 An IS auditor is evaluating a virtual machine (VM)-based architecture used for all programming and testing environments. The production architecture is a three-tier physical architecture. What is the **MOST** important IT control to test to ensure availability and confidentiality of the web application in production?

A. Server configuration has been hardened appropriately.
B. Allocated physical resources are available.
C. System administrators are trained to use the VM architecture.
D. The VM server is included in the disaster recovery plan.

A is the correct answer.

Justification:

A. **The most important control to test in this configuration is the server configuration hardening. It is important to patch known vulnerabilities and to disable all non-required functions before production, especially when production architecture is different from development and testing architecture.**
B. The greatest risk is associated with the difference between the testing and production environments. Ensuring that physical resources are available is a relatively low risk and easily addressed.
C. Virtual machines (VMs) are often used for optimizing programming and testing infrastructure. In this scenario, the development environment (VM architecture) is different from the production infrastructure (physical three-tier). Because the VMs are not related to the web application in production, there is no real requirement for the system administrators to be familiar with a virtual environment.
D. Because the VMs are only used in a development environment and not in production, it may not be necessary to include VMs in the disaster recovery plan.

A5-199 In what capacity would an IS auditor **MOST** likely see a hash function applied?

A. Authentication
B. Identification
C. Authorization
D. Encryption

A is the correct answer.

Justification:

A. **The purpose of a hash function is to produce a "fingerprint" of data that can be used to ensure integrity and authentication. A hash of a password also provides for authentication of a user or process attempting to access resources.**
B. Hash functions are not used for identification. They are used to validate the authenticity of the identity.
C. Hash functions are not typically used to provide authorization. Authorization is provided after the authentication has been established.
D. Hash functions do not encrypt data.

A5-200 The **BEST** filter rule for protecting a network from being used as an amplifier in a denial-of-service attack is to deny all:

A. outgoing traffic with source addresses external to the network.
B. incoming traffic with discernible spoofed IP source addresses.
C. incoming traffic that includes options set in the Internet Protocol.
D. incoming traffic whose destination address belongs to critical hosts.

A is the correct answer.

Justification:

A. **Outgoing traffic with an Internet Protocol (IP) source address different than the internal IP range in the network is invalid. In most of the cases, it signals a denial-of-service attack originated by an internal user or by a previously compromised internal machine; in both cases, applying this filter will stop the infected machine from participating in the attack.**
B. Denying incoming traffic will not prevent an internal machine from participating in an attack on an outside target.
C. Incoming traffic will have the IP options set according to the type of traffic. This is a normal condition.
D. Denying incoming traffic to internal hosts will prevent legitimate traffic.

A5-201 The purpose of a mantrap controlling access to a computer facility is **PRIMARILY** to:

A. prevent piggybacking.
B. prevent toxic gases from entering the data center.
C. starve a fire of oxygen.
D. prevent rapid movement in or out of the facility.

A is the correct answer.

Justification:

A. **The intended purpose of a mantrap controlling access to a computer facility is primarily to prevent piggybacking.**
B. Preventing toxic gases from entering the data center could be accomplished with a single self-closing door.
C. Starving a fire of oxygen could be accomplished with a single self-closing fire door.
D. A rapid exit may be necessary in some circumstances (e.g., a fire).

A5-202 Which of the following should be a concern for an IS auditor reviewing an organization's cloud computing strategy which is based on a software as a service (SaaS) model with an external provider?

A. Workstation upgrades must be performed.
B. Long-term software acquisition costs are higher.
C. Contract with the provider does not include onsite technical support.
D. Incident handling procedures with the provider are not well defined.

D is the correct answer.

Justification:

A. Unless organization workstations are obsolete, upgrading should not be an issue with a software as a service (SaaS) model because most applications running as SaaS use common technologies that allow a user to run the software on different devices.
B. The reduction of software acquisition costs is one of the benefits of SaaS.
C. A SaaS provider does not normally have onsite support for the organization.
D. A SaaS provider does not normally have onsite support for the organization. Therefore, incident handling procedures between the organization and its provider are critical for the detection, communication and resolution of incidents, including effective lines of communication and escalation processes.

A5-203 A company has decided to implement an electronic signature scheme based on a public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The **MOST** significant risk of this approach is:

A. use of the user's electronic signature by another person if the password is compromised.
B. forgery by using another user's private key to sign a message with an electronic signature.
C. impersonation of a user by substitution of the user's public key with another person's public key.
D. forgery by substitution of another person's private key on the computer.

A is the correct answer.

Justification:

A. The user's digital signature is only protected by a password. Compromise of the password would enable access to the signature. This is the most significant risk.
B. Creating a digital signature with another user's private key would indicate that the message came from a different person, and therefore, the true user's credentials would not be forged.
C. Impersonation of a public key would require the modification of the certificate issued by the certificate authority. This is very difficult and least likely.
D. The substitution of another person's private key would not work because the digital signature would be validated with the original user's public key.

A5-204 Which of the following would be **BEST** prevented by a raised floor in the computer machine room?

A. Damage of wires around computers and servers
B. A power failure from static electricity
C. Shocks from earthquakes
D. Water flood damage

A is the correct answer.

Justification:

A. **The primary reason for having a raised floor is to enable ventilation systems, power cables and data cables to be installed underneath the floor. This eliminates the safety and damage risk posed when cables are placed in a spaghetti-like fashion on an open floor.**
B. Static electricity should be avoided in the machine room; therefore, measures such as specially manufactured carpet or shoes would be more appropriate for static prevention than a raised floor.
C. Raised floors do not address shocks from earthquakes. To address earthquakes, anti-seismic architecture would be required to establish a quake-resistant structural framework.
D. Computer equipment needs to be protected against water. However, a raised floor would not prevent damage to the machines in the event of overhead water pipe leakage.

A5-205 A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

A. Introduce a secondary authentication method such as card swipe.
B. Apply role-based permissions within the application system.
C. Have users input the ID and password for each database transaction.
D. Set an expiration period for the database password embedded in the program.

B is the correct answer.

Justification:

A. The issue is user permissions, not authentication; therefore, adding a stronger authentication does not improve the situation.
B. **This is a normal process to allow the application to communicate with the database. Therefore, the best control is to control access to the application and procedures to ensure that access to data is granted based on a user's role.**
C. Having a user input the ID and password for access would provide a better control because a database log would identify the initiator of the activity. However, this may not be efficient because each transaction would require a separate authentication process.
D. It is a good practice to set an expiration date for a password. However, this might not be practical for an ID automatically logged in from the program. Often, this type of password is set not to expire.

A5-206 An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is **MOST** important?

A. The tools used to conduct the test
B. Certifications held by the IS auditor
C. Permission from the data owner of the server
D. An intrusion detection system is enabled

C is the correct answer.

Justification:

A. The choice of tools is important to ensure a valid test and prevent system failure; however, the permission of the owner is most important.
B. Whether the IS auditor holds certifications is not relevant to the effectiveness of the test.
C. The data owner should be informed of the risk associated with a penetration test, the timing of the test, what types of tests are to be conducted and other relevant details.
D. An intrusion detection system is not required for a penetration test.

A5-207 The **GREATEST** benefit of having well-defined data classification policies and procedures is:

A. a more accurate inventory of information assets.
B. a decreased cost of controls.
C. a reduced risk of inappropriate system access.
D. an improved regulatory compliance.

B is the correct answer.

Justification:

A. A more accurate inventory of information assets is a benefit but would not be the greatest benefit of the choices listed.
B. An important benefit of a well-defined data classification process would be to lower the cost of protecting data by ensuring that the appropriate controls are applied with respect to the sensitivity of the data. Without a proper classification framework, some security controls may be greater and, therefore, costlier than is required based on the data classification.
C. Classifying the data may assist in reducing the risk of inappropriate system access, but that would not be the greatest benefit.
D. Improved regulatory compliance would be a benefit; however, achieving a cost reduction would be a greater benefit.

A5-208 Which of the following criteria are **MOST** needed to ensure that log information is admissible in court? Ensure that data have been:

A. independently time stamped.
B. recorded by multiple logging systems.
C. encrypted by the most secure algorithm.
D. verified to ensure log integrity.

D is the correct answer.

Justification:

A. Independent time stamps are a key requirement in logging. This is one method of ensuring log integrity; however, this does not prevent information from being modified.
B. Having multiple logging resources may work to ensure redundancy; however, increased redundancy may not effectively add value to the credibility of log information.
C. The strength of the encryption algorithm may improve data confidentiality; however, this does not necessarily prevent data from being modified.
D. It is important to assure that log information existed at a certain point of time and it has not been altered. Therefore, evidential credibility of log information is enhanced when there is proof that no one has tampered with this information, something typically accomplished by maintaining a documented chain of custody.

A5-209 Which of the following is the **MOST** reliable form of single factor personal identification?

A. Smart card
B. Password
C. Photo identification
D. Iris scan

D is the correct answer.

Justification:

A. There is no guarantee that a smart card is being used by the correct person because it can be shared, stolen, or lost and found.
B. Passwords can be shared and, if written down, carry the risk of discovery.
C. Photo IDs can be forged or falsified.
D. Because no two irises are alike, identification and verification can be done with confidence.

A5-210 Which of the following controls would be **MOST** effective in reducing the risk of loss due to fraudulent online payment requests?

A. Transaction monitoring
B. Protecting web sessions using Secure Sockets Layer
C. Enforcing password complexity for authentication
D. Inputting validation checks on web forms

A is the correct answer.

Justification:

A. **An electronic payment system could be the target of fraudulent activities. An unauthorized user could potentially enter false transactions. By monitoring transactions, the payment processor could identify potentially fraudulent transactions based on the typical usage patterns, monetary amounts, physical location of purchases, and other data that are part of the transaction process.**
B. Using Secure Sockets Layer would help to ensure the secure transmission of data to and from the user's web browser and help to ensure that the end user has reached the correct web site, but this would not prevent fraudulent transactions.
C. Online transactions are not necessarily protected by passwords; for example, credit card transactions are not necessarily protected. The use of strong authentication would help to protect users of the system from fraud by attackers guessing passwords, but transaction monitoring would be the better control.
D. Inputting validation checks on web forms is important to ensure that attackers do not compromise the web site, but transaction monitoring would be the best control.

A5-211 Users are issued security tokens to be used in combination with a personal identification number (PIN) to access the corporate virtual private network. Regarding the PIN, what is the **MOST** important rule to be included in a security policy?

A. Users should not leave tokens where they could be stolen.
B. Users must never keep the token in the same bag as their laptop computer.
C. Users should select a PIN that is completely random, with no repeating digits.
D. Users should never write down their PIN.

D is the correct answer.

Justification:

A. Access to the token is of no value without the personal identification number (PIN); one cannot work without the other.
B. Access to the token is of no value without the PIN; one cannot work without the other.
C. The PIN does not need to be random as long as it is secret.
D. **If a user writes their PIN on a slip of paper, an individual with the token, the slip of paper, and the computer could access the corporate network. A token and the PIN is a two-factor authentication method.**

A5-212 A firewall is being deployed at a new location. Which of the following is the **MOST** important factor in ensuring a successful deployment?

A. Reviewing logs frequently
B. Testing and validating the rules
C. Training a local administrator at the new location
D. Sharing firewall administrative duties

B is the correct answer.

Justification:
A. A regular review of log files would not start until the deployment has been completed.
B. A mistake in the rule set can render a firewall ineffective or insecure. Therefore, testing and validating the rules is the most important factor in ensuring a successful deployment.
C. Training a local administrator may not be necessary if the firewalls are managed from a central location.
D. Having multiple administrators is a good idea, but not the most important for successful deployment.

A5-213 A data center has a badge-entry system. Which of the following is **MOST** important to protect the computing assets in the center?

A. Badge readers are installed in locations where tampering would be noticed.
B. The computer that controls the badge system is backed up frequently.
C. A process for promptly deactivating lost or stolen badges is followed.
D. All badge entry attempts are logged, whether or not they succeed.

C is the correct answer.

Justification:
A. Tampering with a badge reader cannot open the door, so this is irrelevant.
B. The configuration of the system does not change frequently; therefore, frequent backup is not necessary.
C. The biggest risk is from unauthorized individuals who can enter the data center, whether they are employees or not. Thus, having and following a process of deactivating lost or stolen badges is important.
D. Logging the entry attempts is important, but not as important as ensuring that a lost or stolen badge is disabled as quickly as possible.

A5-214 What is the **MOST** prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

A. Malicious code could be spread across the network.
B. The VPN logon could be spoofed.
C. Traffic could be sniffed and decrypted.
D. The VPN gateway could be compromised.

A is the correct answer.

Justification:
A. Virtual private network (VPN) is a mature technology; VPN devices are hard to break. However, when remote access is enabled, malicious code in a remote client could spread to the organization's network. One problem is when the VPN terminates inside the network and the encrypted VPN traffic goes through the firewall. This means that the firewall cannot adequately examine the traffic.
B. A secure VPN solution would use two-factor authentication to prevent spoofing.
C. Sniffing encrypted traffic does not generally provide an attack vector for its unauthorized decryption.
D. A misconfigured or poorly implemented VPN gateway could be subject to attack, but if it is located in a secure subnet, then the risk is reduced.

A5-215 The use of digital signatures:

A. requires the use of a one-time password generator.
B. provides encryption to a message.
C. validates the source of a message.
D. ensures message confidentiality.

C is the correct answer.

Justification:

A. A one-time password generator is not a requirement for using digital signatures.
B. A digital signature provides for integrity and proof of origin for a message but does not address confidentiality.
C. **The use of a digital signature verifies the identity of the sender.**
D. A digital signature does not ensure message confidentiality.

A5-216 The **FIRST** step in a successful attack to a system is:

A. gathering information.
B. gaining access.
C. denying services.
D. evading detection.

A is the correct answer.

Justification:

A. **Successful attacks start by gathering information about the target system. This is done in advance so that the attacker gets to know the target systems and the potential vulnerabilities that can be exploited in the attack.**
B. Once attackers have discovered potential vulnerabilities through information gathering, they will usually attempt to gain access.
C. An attacker will usually launch a denial of service as one of the last steps in the attack.
D. When attackers have gained access and possibly infected the victim with a rootkit, they will delete audit logs and take other steps to hide their tracks.

A5-217 Which of the following methods **BEST** mitigates the risk of disclosing confidential information through the use of social networking sites?

A. Providing security awareness training
B. Requiring a signed acceptable use policy
C. Monitoring the use of social media
D. Blocking access to social media

A is the correct answer.

Justification:

A. **Providing security awareness training is the best method to mitigate the risk of disclosing confidential information on social networking sites. It is important to remember that users may access these services through other means such as mobile phones and home computers; therefore, awareness training is most critical.**
B. Requiring a signed acceptable use policy can be a good control. However, if users are not aware of the risk, then this policy may not be effective.
C. Monitoring the use of social media through the use of a proxy server that tracks the web sites users visit is not an effective control because users may access these services through other means such as mobile phones and home computers.
D. Blocking the use of social media through network controls is not an effective control because users may access these services through other means such as mobile phones and home computers.

A5-218 An IS auditor finds that conference rooms have active network ports. Which of the following would prevent this discovery from causing concern?

A. The corporate network is using an intrusion prevention system.
B. This part of the network is isolated from the corporate network.
C. A single sign-on has been implemented in the corporate network.
D. Antivirus software is in place to protect the corporate network.

B is the correct answer.

Justification:
A. An intrusion prevention system may stop an attack, but it would be far better to restrict the ability of machines in the conference rooms from being able to access the corporate network altogether.
B. If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or by being physically separated.
C. A single sign-on solution is used for access control but would not still leave a risk when unauthorized people have physical access to the corporate network.
D. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

A5-219 When conducting a penetration test of an IT system, an organization should be **MOST** concerned with:

A. the confidentiality of the report.
B. finding all weaknesses on the system.
C. restoring systems to the original state.
D. logging changes made to production systems.

C is the correct answer.

Justification:
A. A penetration test report is a sensitive document because it lists the vulnerabilities of the target system. However, the main requirement for the penetration test team is to restore the system to its original condition.
B. Finding all possible weaknesses is not possible in complex information systems.
C. After the test is completed, the systems must be restored to their original state. In performing the test, changes may have been made to firewall rules, user IDs created, or false files uploaded. These must all be cleaned up before the test is completed.
D. All changes made should be recorded, but the most important concern is to ensure that the changes are reversed at the end of the test.

A5-220 An IS auditor is reviewing a new web-based order entry system the week before it goes live. The IS auditor has identified that the application, as designed, may be missing several critical controls regarding how the system stores customer credit card information. The IS auditor should **FIRST**:

A. determine whether system developers have proper training on adequate security measures.
B. determine whether system administrators have disabled security controls for any reason.
C. verify that security requirements have been properly specified in the project plan.
D. validate whether security controls are based on requirements which are no longer valid.

C is the correct answer.

Justification:

A. While it is important for programmers to understand security, it is more important that the security requirements were properly stated in the project plan.
B. System administrators may have made changes to the controls, but it is assumed that the auditor is reviewing the system as designed a week prior to implementation so the administrators have not yet configured the system.
C. **If there are significant security issues identified by an IS auditor, the first question is whether the security requirements were correct in the project plan. Depending on whether the requirements were included in the plan would affect the recommendations the auditor would make.**
D. It is possible that security requirements will change over time based on new threats or vulnerabilities, but if critical controls are missing, this points toward a faulty design that was based on incomplete requirements.

A5-221 When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

A. Personal firewall
B. Antivirus programs
C. Intrusion detection system
D. Virtual local area network configuration

C is the correct answer.

Justification:

A. Personal firewalls would be later in the defensive strategy, being located on the endpoints.
B. Antivirus programs would be installed on endpoints as well as on the network, but the next layer of defense after a firewall is an intrusion detection system (IDS)/intrusion protection system.
C. **An IDS would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator.**
D. Virtual local area network configurations are not intended to compensate for a compromise of the firewall. They are an architectural good practice.

A5-222 Which of the following is the **BEST** control to mitigate the risk of pharming attacks to an Internet banking application?

A. User registration and password policies
B. User security awareness
C. Use of intrusion detection/intrusion prevention systems
D. Domain name system server security hardening

D is the correct answer.

Justification:

A. User registration and password policies cannot mitigate pharming attacks because they do not prevent manipulation of domain name system (DNS) records.
B. User security awareness cannot mitigate pharming attacks because it does not prevent manipulation of DNS records.
C. The use of intrusion detection/intrusion prevention systems cannot mitigate pharming attacks because they do not prevent manipulation of DNS records.
D. The pharming attack redirects the traffic to an unauthorized web site by exploiting vulnerabilities of the DNS server. To avoid this kind of attack, it is necessary to eliminate any known vulnerability that could allow DNS poisoning. Older versions of DNS software are vulnerable to this kind of attack and should be patched.

A5-223 Which of the following would **MOST** effectively enhance the security of a challenge-response based authentication system?

A. Selecting a more robust algorithm to generate challenge strings
B. Implementing measures to prevent session hijacking attacks
C. Increasing the frequency of associated password changes
D. Increasing the length of authentication strings

B is the correct answer.

Justification:

A. Selecting a more robust algorithm will enhance the security; however, this may not be as important in terms of risk mitigation when compared to man-in-the-middle attacks.
B. Challenge response-based authentication is prone to session hijacking or man-in-the-middle attacks. Security management should be aware of this and engage in risk assessment and control design such as periodic authentication when they employ this technology.
C. Frequently changing passwords is a good security practice; however, the exposures lurking in communication pathways may pose a greater risk.
D. Increasing the length of authentication strings will not prevent man-in-the-middle or session hijacking attacks.

A5-224 When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

A. Using a cryptographic hashing algorithm
B. Enciphering the message digest
C. Calculating a checksum of the transaction
D. Using a sequence number and time stamp

D is the correct answer.

Justification:

A. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity but will not prevent duplicate processing.
B. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the source and integrity of the transaction but will not prevent duplicate processing.
C. A checksum can be used for data integrity but not to prevent duplicate transactions.
D. When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection and could be used to verify that a payment instruction was not duplicated.

A5-225 In wireless communication, which of the following controls allows the receiving device to verify that the received communications have not been altered in transit?

A. Device authentication and data origin authentication
B. Wireless intrusion detection and intrusion prevention systems
C. The use of cryptographic hashes
D. Packet headers and trailers

C is the correct answer.

Justification:

A. Device authentication and data origin authentication allow wireless endpoints to authenticate each other to prevent man-in-the-middle attacks and masquerading.
B. Wireless intrusion detection and intrusion prevention systems have the ability to detect misconfigured devices and rogue devices and detect and possibly stop certain types of attacks.
C. Calculating cryptographic hashes for wireless communications allows the receiving device to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks.
D. Packet headers and trailers alone do not ensure that the content has not been altered because an attacker could alter both the data and the trailer.

A5-226 An organization is planning to replace its wired networks with wireless networks. Which of the following would **BEST** secure the wireless network from unauthorized access?

A. Implement Wired Equivalent Privacy.
B. Permit access to only authorized media access control addresses.
C. Disable open broadcast of service set identifiers.
D. Implement Wi-Fi Protected Access 2.

D is the correct answer.

Justification:

A. Wired Equivalent Privacy can be cracked within minutes. WEP uses a static key that has to be communicated to all authorized users, thus management is difficult. Also, there is a greater vulnerability if the static key is not changed at regular intervals.
B. The practice of allowing access based on media access control is not a solution because MAC addresses can be spoofed by attackers to gain access to the network.
C. Disabling open broadcast of service set identifiers is not an effective access control because many tools can detect a wireless access point that is not broadcasting.
D. Wi-Fi Protected Access (WPA) 2 implements most of the requirements of the IEEE 802.11i standard. The Advanced Encryption Standard used in WPA2 provides better security. Also, WPA2 supports both the Extensible Authentication Protocol and the pre-shared secret key authentication model.

A5-227 An IS auditor is reviewing a software-based firewall configuration. Which of the following represents the **GREATEST** vulnerability?

A. An implicit deny rule as the last rule in the rule base.
B. Installation on an operating system configured with default settings.
C. Rules permitting or denying access to systems or networks.
D. Configuration as a virtual private network endpoint.

B is the correct answer.

Justification:

A. Configuring a firewall with an implicit deny rule is common practice.
B. Default settings of most equipment—including operating systems—are often published and provide an intruder with predictable configuration information, which allows easier system compromise. To mitigate this risk, firewall software should be installed on a system using a hardened operating system that has limited functionality, providing only the services necessary to support the firewall software.
C. A firewall configuration should have rules allowing or denying access according to policy.
D. A firewall is often set up as the endpoint for a virtual private network.

A5-228 The **GREATEST** risk from an improperly implemented intrusion prevention system is:

A. too many alerts for system administrators to verify.
B. decreased network performance due to additional traffic.
C. blocking of critical systems or services due to false triggers.
D. reliance on specialized expertise within the IT organization.

C is the correct answer.

Justification:
A. A number of false positives may cause excessive administrator workload, but this is a relatively minor risk.
B. The intrusion prevention system will not generate any traffic that would impact network performance.
C. **An IPS prevents a connection or service based on how it is programmed to react to specific incidents. If the IPS is triggered based on incorrectly defined or nonstandard behavior, it may block the service or connection of a critical internal system.**
D. Configuring an IPS can take months of learning what is and what is not acceptable behavior, but this does not require specialized expertise.

A5-229 When reviewing a digital certificate verification process, which of the following findings represents the **MOST** significant risk?

A. There is no registration authority for reporting key compromises.
B. The certificate revocation list is not current.
C. Digital certificates contain a public key that is used to encrypt messages and verify digital signatures.
D. Subscribers report key compromises to the certificate authority.

B is the correct answer.

Justification:
A. The certificate authority (CA) can assume the responsibility if there is no registration authority.
B. **If the certificate revocation list is not current, there could be a digital certificate that is not revoked that could be used for unauthorized or fraudulent activities.**
C. Digital certificates contain a public key that is used to encrypt messages and verify digital signatures; therefore, this is not a risk.
D. Subscribers reporting key compromises to the CA is not a risk because reporting this to the CA enables the CA to take appropriate action.

A5-230 When using a digital signature, the message digest is computed by the:

A. sender only.
B. receiver only.
C. sender and receiver both.
D. certificate authority.

C is the correct answer.

Justification:
A. The message digest must be computed by the sender and the receiver to ensure message integrity.
B. The receiver will compute a digest of the received message to verify integrity of the received message.
C. **A digital signature is an electronic identification of a person or entity. It is created by using asymmetric encryption. To verify integrity of data, the sender uses a cryptographic hashing algorithm against the entire message to create a message digest to be sent along with the message. Upon receipt of the message, the receiver will recompute the hash using the same algorithm.**
D. The certificate authority (CA) issues certificates that link the public key with its owner. The CA does not compute digests of the messages to be communicated between the sender and receiver.

A5-231 Which of the following would 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 to encapsulate transaction content
D. Digitally signing the transaction with the source's private key

D is the correct answer.

Justification:

A. Because they are a "shared secret" between the user and the system itself, passwords are considered a weaker means of authentication.
B. Encrypting the transaction with the recipient's public key will provide confidentiality for the information but will not verify the source.
C. Using a portable document format will protect the integrity of the content but not necessarily authorship.
D. A digital signature is an electronic identification of a person, created by using a public key algorithm, to verify the identity of the source of a transaction and the integrity of its content to a recipient.

A5-232 An organization has established a guest network for visitor access. Which of the following should be of **GREATEST** concern to an IS auditor?

A. A login screen is not displayed for guest users.
B. The guest network is not segregated from the production network.
C. Guest users who are logged in are not isolated from each other.
D. A single factor authentication technique is used to grant access.

B is the correct answer.

Justification:

A. Using a web captive portal, which displays a login screen in the user's web browser, is a good practice to authenticate guests. However, if the guest network is not segregated from the production network, users could introduce malware and potentially gain inappropriate access to systems and information.
B. The implication of this is that guests have access to the organization's network. Allowing untrusted users to connect to the organization's network could introduce malware and potentially allow these individuals inappropriate access to systems and information.
C. There are certain platforms in which it is allowable for guests to interact with one another. Also, guests could be warned to use only secured systems and a policy covering interaction among guests could be created.
D. Although a multifactor authentication technique is preferred, a single-factor authentication method should be adequate if properly implemented.

A5-233 Which of the following provides the **GREATEST** assurance for database password encryption?

A. Secure hash algorithm-256
B. Advanced encryption standard
C. Secure Shell
D. Triple data encryption standard

B is the correct answer.

Justification:

A. Hashing functions are often used to protect passwords, but hashing is not encryption.
B. The use of advanced encryption standard (AES) is a secure encryption algorithm that is appropriate for encrypting passwords.
C. Secure Shell may encrypt passwords that are being transmitted but does not encrypt data at rest.
D. Triple Data Encryption Standard is a valid encryption method; however, AES is a stronger and more recent encryption algorithm.

A5-234 The reason a certification and accreditation process is performed on critical systems is to ensure that:

A. Security compliance has been technically evaluated
B. Data have been encrypted and are ready to be stored
C. The systems have been tested to run on different platforms
D. The systems have followed the phases of a waterfall model

A is the correct answer.

Justification:

A. **Certified and accredited systems are systems that have had their security compliance technically evaluated for running in a specific environment and configuration.**
B. Certification tests security functionality, including encryption where that is required, but that is not the primary objective of the certification and accreditation (C&A) process.
C. Certified systems are evaluated to run in a specific environment.
D. A waterfall model is a software development methodology and not a reason for performing a C&A process.

A5-235 A perpetrator looking to gain access to and gather information about encrypted data being transmitted over a network would **MOST** likely use:

A. eavesdropping.
B. spoofing.
C. traffic analysis.
D. masquerading.

C is the correct answer.

Justification:

A. In eavesdropping, which is a passive attack, the intruder gathers the information flowing through the network with the intent of acquiring message contents for personal analysis or for third parties. Encrypted traffic is generally protected against eavesdropping
B. Spoofing is an active attack. In spoofing, a user receives an email that appears to have originated from one source when it actually was sent from another source.
C. **In traffic analysis, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, the intruder is able to guess the type of communication taking place. This typically is used when messages are encrypted, and eavesdropping would not yield any meaningful results.**
D. In masquerading, the intruder presents an identity other than the original identity. This is an active attack.

A5-236 A hotel has placed a PC in the lobby to provide guests with Internet access. Which of the following presents the **GREATEST** risk for identity theft?

A. Web browser cookies are not automatically deleted.
B. The computer is improperly configured.
C. System updates have not been applied on the computer.
D. Session time out is not activated.

D is the correct answer.

Justification:
A. If web browser cookies are not automatically deleted, it might be possible to determine the web sites that a user has accessed. However, if sessions do not time out, it is easier for identity theft to occur.
B. If the PC is not configured properly and does not have antivirus software installed, there could be a risk of virus or malware infection. This could cause identity theft. However, if sessions do not time out, it is easier for identity theft to occur.
C. If system updates have not been applied, there could be a greater risk of virus or malware infection. This could cause identity theft. However, if sessions do not time out, it is easier for identity theft to occur.
D. If an authenticated session is inactive and unattended, it can be hijacked and used for illegal purposes. It might then be difficult to establish the intruder because a legitimate session was used.

A5-237 The **MOST** effective biometric control system is the one with:

A. the highest equal-error rate.
B. the lowest equal-error rate.
C. a false-rejection rate equal to the false-acceptance rate.
D. a false-rejection rate equal to the failure-to-enroll rate.

B is the correct answer.

Justification:
A. The biometric that has the highest equal-error rate (EER) is the most ineffective.
B. The EER of a biometric system denotes the percent at which the false-acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective.
C. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER.
D. Failure-to-enroll rate (FER) is an aggregate measure of FRR.

A5-238 Which of the following is a form of two-factor user authentication?

A. A smart card and personal identification number
B. A unique User ID and complex, non-dictionary password
C. An iris scan and a fingerprint scan
D. A magnetic-strip card and a proximity badge

A is the correct answer.

Justification:
A. A smart card is something that a user has, while a personal identification number paired with the card is something the user knows. This is an example of two-factor authentication.
B. Both an ID and a password are something the user knows, so this pairing provides single-factor user authentication regardless of complexity.
C. Both an iris scan and a fingerprint scan are something the user is, so this pairing is not a basis for two-factor user authentication.
D. Both a magnetic card and a proximity badge are examples of something a user has, so these are not adequate for two-factor authentication.

A5-239 An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be **MOST** concerned that:

A. Non-personalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
B. access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
C. card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
D. the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

A is the correct answer.

Justification:

A. **Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequate to trust unknown external people by allowing them to write down their alleged name without proof (e.g., identity card, driver's license).**
B. Having the name and address of the organization on the card may be a concern because a malicious finder could use a lost or stolen card to enter the organization's premises.
C. Separating card issuance from technical rights management is a method to ensure the proper segregation of duties so that no single person can produce a functioning card for a restricted area within the organization's premises. The long lead time is an inconvenience but not a serious audit risk.
D. System failure of the card programming device would normally not mean that the readers do not function anymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

A5-240 When reviewing the procedures for the disposal of computers, which of the following should be the **GREATEST** concern for the IS auditor?

A. Hard disks are overwritten several times at the sector level but are not reformatted before leaving the organization.
B. All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
C. Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
D. The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

B is the correct answer.

Justification:

A. Overwriting a hard disk at the sector level would completely erase data, directories, indices and master file tables. Reformatting is not necessary because all contents are destroyed. Overwriting several times makes useless some forensic measures, which are able to reconstruct former contents of newly overwritten sectors by analyzing special magnetic features of the platter's surface.
B. **Deleting and formatting only marks the sectors that contained files as being free. Publicly available tools are sufficient for someone to reconstruct data from hard drives prepared this way.**
C. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted. Reconstructing data would be extremely expensive because all analysis must be performed under a clean room atmosphere and is only possible within a short time frame or until the surface is corroded.
D. Data reconstruction from shredded hard disks is virtually impossible, especially when the scrap is mixed with other metal parts. If the transport can be secured and the destruction be proved as described in the option, this is a valid method of disposal.

A5-241 A new business application requires deviation from the standard configuration of the operating system (OS). What activity should the IS auditor recommend to the security manager as a **FIRST** response?

A. Initial rejection of the request because it is against the security policy
B. Approval of the exception to policy to meet business needs
C. Assessment of the risk and identification of compensating controls
D. Revision of the OS baseline configuration

C is the correct answer.

Justification:

A. The security policy may be waived with management approval to meet business requirements; it is not up to the security manager to refuse the deviation.
B. The security manager may make a case for deviation from the policy, but this should be based on a risk assessment and compensating controls. The deviation itself should be approved in accordance with a defined exception handling process.
C. **Before approving any exception, the security manager should first check for compensating controls and assess the possible risk due to deviation.**
D. Updating or revising the baseline configuration is not associated with requests for deviations.

A5-242 An organization has created a policy that defines the types of web sites that users are forbidden to access. What is the **MOST** effective technology to enforce this policy?

A. Stateful inspection firewall
B. Web content filter
C. Web cache server
D. Proxy server

B is the correct answer.

Justification:

A. A stateful inspection firewall is of little help in filtering web traffic because it does not review the content of the web site, nor does it take into consideration the site's classification.
B. **A web content filter accepts or denies web communications according to the configured rules. To help the administrator properly configure the tool, organizations and vendors have made available uniform resource locator blacklists and classifications for millions of web sites.**
C. A web cache server is designed to improve the speed of retrieving the most common or recently visited web pages.
D. A proxy server is incorrect because a proxy server services the request of its clients by forwarding requests to other servers. Many people incorrectly use proxy server as a synonym of web proxy server even though not all web proxy servers have content filtering capabilities.

A5-243 Which of the following specifically addresses how to detect cyberattacks against an organization's IT systems and how to recover from an attack?

A. An incident response plan
B. An IT contingency plan
C. A business continuity plan
D. A continuity of operations plan

A is the correct answer.

Justification:

A. **The incident response plan (IRP) determines the information security responses to incidents such as cyberattacks on systems and/or networks. This plan establishes procedures to enable security personnel to identify, mitigate and recover from malicious computer incidents such as unauthorized access to a system or data, denial-of-service or unauthorized changes to system hardware or software.**
B. The IT contingency plan addresses IT system disruptions and establishes procedures for recovering from a major application or general support system failure. The contingency plan deals with ways to recover from an unexpected failure, but it does not address the identification or prevention of cyberattacks.
C. The business continuity plan (BCP) addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. While a cyberattack could be severe enough to require use of the BCP, the IRP would be used to determine which actions should be taken—both to stop the attack as well as to resume normal operations after the attack.
D. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and contains procedures to sustain these functions at an alternate site for a short time period.

A5-244 The cryptographic hash sum of a message is recalculated by the receiver. This is to ensure:

A. the confidentiality of the message.
B. nonrepudiation by the sender.
C. the authenticity of the message.
D. the integrity of data transmitted by the sender.

D is the correct answer.

Justification:

A. A hash function ensures integrity of a message; encrypting with a secret key provides confidentiality.
B. Signing the message with the private key of the sender ensures nonrepudiation and authenticity.
C. Authenticity of the message is provided by the digital signature.
D. **If the hash sum is different from what is expected, it implies that the message has been altered. This is an integrity test.**

A5-245 The computer security incident response team of an organization disseminates detailed descriptions of recent threats. An IS auditor's **GREATEST** concern should be that the users may:

A. use this information to launch attacks.
B. forward the security alert.
C. implement individual solutions.
D. fail to understand the threat.

A is the correct answer.

Justification:

A. **An organization's computer security incident response team (CSIRT) should disseminate recent threats, security guidelines and security updates to the users to assist them in understanding the security risk of errors and omissions. However, this introduces the risk that the users may use this information to launch attacks, directly or indirectly. An IS auditor should ensure that the CSIRT is actively involved with users to assist them in mitigation of risk arising from security failures and to prevent additional security incidents resulting from the same threat.**
B. Forwarding the security alert is not harmful to the organization.
C. Implementing individual solutions is unlikely and inefficient, but not a serious risk.
D. Users failing to understand the threat would not be a serious concern.

A5-246 Which of the following would be an indicator of the effectiveness of a computer security incident response team?

A. Financial impact per security incident
B. Number of security vulnerabilities that were patched
C. Percentage of business applications that are being protected
D. Number of successful penetration tests

A is the correct answer.

Justification:

A. **The most important indicator is the financial impact per security incident. It may not be possible to prevent incidents entirely, but the team should be able to limit the cost of incidents through a combination of effective prevention, detection and response.**
B. Patching of security vulnerabilities is important but not a direct responsibility of the computer security incident response team (CSIRT).
C. The CSIRT is not responsible for the protection of systems. That is the responsibility of the security team.
D. The number of penetration tests measures the effectiveness of the security team and the patch management process, but not the effectiveness of the CSIRT.

A5-247 A benefit of quality of service is that the:

A. entire network's availability and performance will be significantly improved.
B. telecom carrier will provide the company with accurate service-level compliance reports.
C. participating applications will have bandwidth guaranteed.
D. communications link will be supported by security controls to perform secure online transactions.

C is the correct answer.

Justification:

A. Quality of service (QoS) will not guarantee that the communication itself will be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved.
B. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports.
C. **The main function of QoS is to optimize network performance by assigning priority to business applications and end users through the allocation of dedicated parts of the bandwidth to specific traffic.**
D. Even when QoS is integrated with firewalls, virtual private networks (VPNs), encryption tools and others, the tool itself is not intended to provide security controls.

A5-248 Which of the following procedures would **MOST** effectively detect the loading of illegal software packages onto a network?

A. The use of diskless workstations
B. Periodic checking of hard drives
C. The use of current antivirus software
D. Policies that result in instant dismissal if violated

B is the correct answer.

Justification:

A. Diskless workstations act as a preventive control and are not totally effective in preventing users from accessing illegal software over the network.
B. **The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded onto the network.**
C. Antivirus software will not necessarily identify illegal software, unless the software contains a virus.
D. Policies are a preventive control to lay out the rules about loading the software, but will not detect the actual occurrence.

A5-249 An online stock trading firm is in the process of implementing a system to provide secure email exchange with its customers. What is the **BEST** option to ensure confidentiality, integrity and nonrepudiation?

A. Symmetric key encryption
B. Digital signatures
C. Message digest algorithms
D. Digital certificates

D is the correct answer.

Justification:

A. Symmetric key encryption uses a single pass phrase to encrypt and decrypt the message. While this type of encryption is strong, it suffers from the inherent problem of needing to share the pass phrase in a secure manner and does not address integrity and nonrepudiation.
B. Digital signatures provide message integrity and nonrepudiation; however, confidentiality is not provided.
C. Message digest algorithms are a way to design hashing functions to verify the integrity of the message/data. Message digest algorithms do not provide confidentiality or nonrepudiation.
D. A digital certificate contains the public key and identifying information about the owner of the public key. The associated private key pair is kept secret with the owner. These certificates are generally verified by a trusted authority, with the purpose of associating a person's identity with the public key. Email confidentiality and integrity are obtained by following the public key-private key encryption. With the digital certificate verified by the trusted third party, nonrepudiation of the sender is obtained.

A5-250 An IS auditor reviewing the authentication controls of an organization should be **MOST** concerned if:

A. user accounts are not locked out after five failed attempts.
B. passwords can be reused by employees within a defined time frame.
C. system administrators use shared login credentials.
D. password expiration is not automated.

C is the correct answer.

Justification:

A. If user accounts are not locked after multiple failed attempts, a brute force attack could be used to gain access to the system. While this is a risk, a typical user would have limited system access compared to an administrator.
B. The reuse of passwords is a risk. However, the use of shared login credentials by administrators is a more severe risk.
C. The use of shared login credentials makes accountability impossible. This is especially a risk with privileged accounts.
D. If password expiration is not automated, it is most likely that employees will not change their passwords regularly. However, this is not as serious as passwords being shared, and the use of shared login credentials by administrators is a more severe risk.

A5-251 The IS auditor is reviewing the implementation of a storage area network (SAN). The SAN administrator indicates that logging and monitoring is active, hard zoning is used to isolate data from different business units and all unused SAN ports are disabled. The administrator implemented the system, performed and documented security testing during implementation, and is the only user with administrative rights to the system. What should the IS auditor's initial determination be?

A. There is no significant potential risk.
B. Soft zoning presents a potential risk.
C. Disabling of unused ports presents a potential risk.
D. The SAN administrator presents a potential risk.

D is the correct answer.

Justification:
A. While the storage area network (SAN) may have been implemented with good controls, there is risk created by the combination of roles held by the SAN administrator.
B. Hard zoning is more secure than soft zoning.
C. Unused ports should generally be disabled to increase security.
D. The potential risk in this scenario is posed by the SAN administrator. One concern is having a "single point of failure." Because only one administrator has the knowledge and access required to administer the system, the organization is susceptible to risk. For example, if the SAN administrator decided to quit unexpectedly, or was otherwise unavailable, the company may not be able to adequately administer the SAN. In addition, having a single administrator for a large, complex system such as a SAN also presents a segregation of duties risk. The organization currently relies entirely on the SAN administrator to implement, maintain, and validate all security controls; this means that the SAN administrator could modify or remove those controls without detection.

A5-252 Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the **MOST** serious?

A. Sensitive data might be read by operators.
B. Data might be amended without authorization.
C. Unauthorized report copies might be printed.
D. Output might be lost in the event of system failure.

C is the correct answer.

Justification:
A. Operators often have high-level access as a necessity to perform their job duties. To the extent that this is a risk, it exists for any form of non-local printing and is not specifically tied to spooled reports.
B. Data on spool files are no easier to amend without authority than any other file.
C. Spooling for offline printing may enable additional copies to be printed unless adequate safeguards exist as compensating controls.
D. Loss of data at the spooler level would only require reprinting.

A5-253 Web and email filtering tools are valuable to an organization **PRIMARILY** because they:

A. protect the organization from viruses and nonbusiness materials.
B. maximize employee performance.
C. safeguard the organization's image.
D. assist the organization in preventing legal issues.

A is the correct answer.

Justification:

A. **The main reason for investing in web and email filtering tools is that they significantly reduce risk related to viruses, spam, mail chains, recreational surfing and recreational email.**
B. Maximizing employee performance could be true in some circumstances (i.e., it would need to be implemented along with an awareness program so that employee performance can be significantly improved). However, the primary benefit is protecting the organization from viruses and nonbusiness activity.
C. Safeguarding the organization's image is a secondary benefit.
D. Preventing legal issues is important, but not the primary reason for filtering.

A5-254 Which of the following types of firewalls provide the **GREATEST** degree and granularity of control?

A. Screening router
B. Packet filter
C. Application gateway
D. Circuit gateway

C is the correct answer.

Justification:

A. Screening routers and packet filters work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4 and not from higher levels.
B. A packet filter works at too low of a level of the communication stack to provide granular control.
C. **The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has a Hypertext Transmission Protocol (HTTP) proxy that acts as an intermediary between externals and internals but is specifically for HTTP. This means that it not only checks the packet Internet Protocol (IP) addresses (Open Systems Interconnection [OSI] Layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (OSI Layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the other choices.**
D. A circuit gateway is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that, during an external access, instead of opening a single connection to the internal server, two connections are established—one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. OSI Layers 3 and 4 (IP and Transmission Control Protocol) and some general features from higher protocols are used to perform these tasks.

A5-255 After installing a network, an organization implemented a vulnerability assessment tool = to identify possible weaknesses. Which type of reporting poses the **MOST** serious risk associated with such tools?

A. Differential
B. False-positive
C. False-negative
D. Less-detail

C is the correct answer.

Justification:

A. Differential reporting function provided by this tool compares scan results over a period of time.
B. False-positive reporting is one in which the system falsely reports a vulnerability. Controls may be in place, but are evaluated as weak, which should prompt a rechecking of the controls.
C. False-negative reporting on weaknesses means the control weaknesses in the network are not identified and, therefore, may not be addressed, leaving the network vulnerable to attack.
D. Less-detail reporting would require additional tools or analysis to determine the existence and severity of vulnerabilities.

A5-256 Which of the following is the **MOST** reliably effective method for dealing with the spread of a network worm that exploits vulnerability in a protocol?

A. Install the latest vendor security patches immediately.
B. Block the protocol traffic in the perimeter firewall.
C. Block the protocol traffic between internal network segments.
D. Stop the services that the protocol uses.

D is the correct answer.

Justification:

A. Installing the latest patches will improve the situation only if a patch has been released that addresses the particular vulnerability in the protocol. Also, patches should not be installed prior to testing, because patching systems can create new vulnerabilities or impact performance.
B. Blocking the protocol on the perimeter does not stop the worm from spreading if it is introduced via portable media.
C. Blocking the protocol helps to slow the spread, but also prohibits any software that uses it from working between segments.
D. Stopping the services is the most effective way to prevent a worm from spreading, because it directly addresses the means of propagation at the lowest practical level.

A5-257 An IS auditor is reviewing an organization's controls related to email encryption. The company's policy states that all sent email must be encrypted to protect the confidentiality of the message because the organization shares nonpublic information through email. In a public-key infrastructure implementation properly configured to provide confidentiality, email is:

A. encrypted with the sender's private key and decrypted with the sender's public key.
B. encrypted with the recipient's private key and decrypted with the sender's private key.
C. encrypted with the sender's private key and decrypted with the recipient's private key.
D. encrypted with the recipient's public key and decrypted with the recipient's private key.

D is the correct answer.

Justification:

A. Encrypting a message with the sender's private key and decrypting it with the sender's public key ensures that the message came from the sender; however, it does not guarantee message confidentiality. With public key infrastructure, a message encrypted with a private key must be decrypted with the responding public key, and vice versa.
B. The sender would not have access to the receiver's private key.
C. A message encrypted with the sender's private key could not be decrypted using the recipient's private key.
D. Encrypting a message with the recipient's public key and decrypting it with the recipient's private key ensures message confidentiality, because only the intended recipient has the correct private key to decrypt the message.

A5-258 Which of the following types of firewalls would **BEST** protect a network from an Internet attack?

A. Screened subnet firewall
B. Application filtering gateway
C. Packet filtering router
D. Circuit-level gateway

A is the correct answer.

Justification:

A. A screened subnet firewall would provide the best protection. The screening router can be a commercial router or a node with routing capabilities and the ability to allow or avoid traffic between nets or nodes based on addresses, ports, protocols, interfaces, etc. The subnet would isolate Internet-based traffic from the rest of the corporate network.
B. Application-level gateways are mediators between two entities that want to communicate, also known as proxy gateways. The application level (proxy) works at the application level, not just at a packet level. This would be the best solution to protect an application but not a network.
C. A packet filtering router examines the header of every packet or data traveling between the Internet and the corporate network. This is a low-level control.
D. A circuit level gateway, such as a Socket Secure server, will protect users by acting as a proxy but is not the best defense for a network.

A5-259 Neural networks are effective in detecting fraud because they can:

A. discover new trends because they are inherently linear.
B solve problems where large and general sets of training data are not obtainable.
C address problems that require consideration of a large number of input variables.
D. make assumptions about the shape of any curve relating variables to the output.

C is the correct answer.

Justification:
A. Neural networks are inherently nonlinear.
B. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.
C. Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends.
D. Neural networks make no assumption about the shape of any curve relating variables to the output.

A5-260 Which of the following **BEST** encrypts data on mobile devices?

A. Elliptical curve cryptography
B. Data encryption standard
C. Advanced encryption standard
D. The Blowfish algorithm

A is the correct answer.

Justification:
A. Elliptical curve cryptography (ECC) requires limited bandwidth resources and is suitable for encrypting mobile devices.
B. Data encryption standard uses less processing power when compared with advanced encryption standard (AES), but ECC is more suitable for encrypting data on mobile devices.
C. AES is a symmetric algorithm and has the problem of key management and distribution. ECC is an asymmetric algorithm and is better suited for a mobile environment.
D. The use of the Blowfish algorithm consumes too much processing power.

A5-261 Confidentiality of transmitted data can best be delivered by encrypting the:

A. Message digest with the sender's private key.
B. Session key with the sender's public key.
C. Messages with the receiver's private key.
D. Session key with the receiver's public key.

D is the correct answer.

Justification:
A. This will ensure authentication and nonrepudiation.
B. This will make the message accessible to only the sender.
C. A message encrypted with a receiver's private key could be decrypted by anyone using the receiver's public key.
D. This will ensure that the session key can only be obtained using the receiver's private key, retained by the receiver.

A5-262 The risk of dumpster diving is **BEST** mitigated by:

A. Implementing security awareness training.
B. Placing shred bins in copy rooms.
C. Developing a media disposal policy.
D. Placing shredders in individual offices.

A is the correct answer.

Justification:

A. **Dumpster diving is used to steal documents or computer media that were not properly discarded. Users should be educated to know the risk of carelessly discarding sensitive documents and other items.**
B. The shred bins may not be properly used if users are not aware of proper security techniques.
C. A media disposal policy is a good idea; however, if users are not aware of the policy it may not be effective.
D. The shredders may not be properly used if users are not aware of proper security techniques.

A5-263 An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the **GREATEST** concern to an IS auditor reviewing the firewall security architecture?

A. A Secure Sockets Layer has been implemented for user authentication and remote administration of the firewall.
B. Firewall policies are updated on the basis of changing requirements.
C Inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
D. The firewall is placed on top of the commercial operating system with all default installation options.

D is the correct answer.

Justification:

A. Using Secure Sockets Layer for firewall administration is important because changes in user and supply chain partners' roles and profiles will be dynamic.
B. It is appropriate to maintain the firewall policies as needed.
C. It is prudent to block all inbound traffic to an extranet unless permitted.
D. **The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached, that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risk of vulnerabilities and exploits.**

A5-264 An organization is proposing to establish a wireless local area network (WLAN). Management asks the IS auditor to recommend security controls for the WLAN. Which of the following would be the **MOST** appropriate recommendation?

A. Physically secure wireless access points to prevent tampering.
B. Use service set identifiers that clearly identify the organization.
C. Encrypt traffic using the Wired Equivalent Privacy mechanism.
D. Implement the Simple Network Management Protocol to allow active monitoring.

A is the correct answer.

Justification:

A. **Physically securing access points such as wireless routers, as well as preventing theft, addresses the risk of malicious parties tampering with device settings. If access points can be physically reached, it is often a simple matter to restore weak default passwords and encryption keys, or to totally remove authentication and encryption from the network.**
B. Service set identifiers should not be used to identify the organization because hackers can associate the wireless local area network with a known organization, and this increases both their motivation to attack and, potentially, the information available to do so.
C. The original Wired Equivalent Privacy security mechanism has been demonstrated to have a number of exploitable weaknesses. The more recently developed Wi-Fi Protected Access and Wi-Fi Protected Access 2 standards represent considerably more secure means of authentication and encryption.
D. Installing Simple Network Management Protocol on wireless access points can actually open up security vulnerabilities. If SNMP is required at all, then SNMP v3, which has stronger authentication mechanisms than earlier versions, should be deployed.

A5-265 Which of the following situations would increase the likelihood of fraud?

A. Application programmers are implementing changes to production programs.
B. Administrators are implementing vendor patches to vendor-supplied software without following change control procedures.
C. Operations support staff members are implementing changes to batch schedules.
D. Database administrators are implementing changes to data structures.

A is the correct answer.

Justification:

A. **Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data.**
B. The lack of change control is a serious risk—but if the changes are only vendor-supplied patches to vendor software then the risk is minimal.
C. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data unless jobs are run in the wrong sequence.
D. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

A5-266 A consulting firm has created a File Transfer Protocol (FTP) site for the purpose of receiving financial data and has communicated the site's address, user ID and password to the financial services company in separate email messages. The company is to transmit its data to the FTP site after manually encrypting the data. The IS auditor's **GREATEST** concern with this process is that:

A. The users may not remember to manually encrypt the data before transmission.
B. The site credentials were sent to the financial services company via email.
C. Personnel at the consulting firm may obtain access to sensitive data.
D. The use of a shared user id to the ftp site does not allow for user accountability.

A is the correct answer.

Justification:
A. **If the data is not encrypted, an unauthorized external party may download sensitive company data.**
B. Even though the possibility exists that the logon information was captured from the emails, data should be encrypted, so the theft of the data would not allow the attacker to read it.
C. Some of the employees at the consulting firm will have access to the sensitive data and the consulting firm must have procedures in place to protect the data.
D. Tracing accountability is of minimal concern compared to the compromise of sensitive data.

A5-267 Java applets and Active X controls are distributed programs that execute in the background of a client web browser. This practice is considered reasonable when:

A. A firewall exists.
B. A secure web connection is used.
C. The source of the executable file is certain.
D. The host web site is part of the organization.

C is the correct answer.

Justification:
A. There should always be a firewall on an Internet connection; however, whether to allow active models is a decision made depending on the source of the module.
B. A secure web connection provides confidentiality. Neither a secure web connection nor a firewall can identify an executable file as friendly.
C. **Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere.**
D. Hosting the web site as part of the organization is impractical. The client will accept the program if the parameters are established to do so.

A5-268 Which of the following controls will **MOST** effectively detect the presence of bursts of errors in network transmissions?

A. Parity check
B. Echo check
C. Block sum check
D. Cyclic redundancy check

D is the correct answer.

Justification:

A. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant.
B. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.
C. A block sum check is a form of parity checking and has a low level of reliability.
D. The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free. In this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and double-bit errors.

A5-269 Which of the following types of transmission media provide the **BEST** security against unauthorized access?

A. Copper wire
B. Shielded twisted pair
C. Fiber-optic cables
D. Coaxial cables

C is the correct answer.

Justification:

A. Twisted pair, coaxial and copper wire traffic can be monitored with inexpensive equipment.
B. Twisted pair cabling is a form of copper wire, and while shielding affords some degree of protection from interference, it does not improve security against unauthorized access.
C. Fiber-optic cables have proven to be more secure and more difficult to tap than the other media.
D. Coaxial cable can be monitored with relative ease.

A5-270 Which of the following is the **BEST** audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

A. Review the parameter settings.
B. Interview the firewall administrator.
C. Review the actual procedures.
D. Review the device's log file for recent attacks.

A is the correct answer.

Justification:

A. A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation.
B. An interview with the firewall administrator will not ensure that the firewall is configured correctly.
C. Reviewing the actual procedures is good but will not ensure that the firewall rules are correct and compliant with policy.
D. Recent attacks may indicate problems with the firewall but will not ensure that it is correctly configured.

A5-271 An IS auditor is reviewing the network infrastructure of a call center and determines that the internal telephone system is based on Voice-over Internet Protocol technology. Which of the following is the **GREATEST** concern?

A. Voice communication uses the same equipment that is used for data communication.
B. Ethernet switches are not protected by uninterrupted power supply units.
C. Voice communication is not encrypted on the local network.
D. The team that supports the data network also is responsible for the telephone system.

B is the correct answer.

Justification:

A. Voice-over Internet Protocol (VoIP) telephone systems use the local area network (LAN) infrastructure of a company for communication, which can save on wiring cost and simplify both the installation and support of the telephone system. This use of shared infrastructure is a benefit of VoIP and therefore is not a concern.
B. **VoIP telephone systems use the LAN infrastructure of a company for communication, typically using Ethernet connectivity to connect individual phones to the system. Most companies have a backup power supply for the main servers and systems, but typically do not have uninterrupted power supply units for the LAN switches. In the case of even a brief power outage, not having backup power on all network devices makes it impossible to send or receive phone calls, which is a concern, particularly in a call center.**
C. VoIP devices do not normally encrypt the voice traffic on the local network, so this is not a concern. Typically, a VoIP phone system connects to a telephone company voice circuit, which would not normally be encrypted. If the system uses the Internet for connectivity, then encryption is required.
D. VoIP telephone systems use the LAN infrastructure of a company for communication, so the personnel who support and maintain that infrastructure are now responsible for both the data and voice network by default. Therefore, this would not be a concern.

A5-272 Which of the following would **BEST** ensure continuity of a wide area network across the organization?

A. Built-in alternative routing
B. Complete full system backup daily
C. A repair contract with a service provider
D. A duplicate machine alongside each server

A is the correct answer.

Justification:

A. **Alternative routing would ensure that the network would continue if a communication device fails or if a link is severed because message rerouting could be automatic.**
B. System backup will not afford protection for a networking failure.
C. The repair contract will almost always result in some lost time and is not as effective as permanent alternative routing.
D. Standby servers will not provide continuity if a link is severed.

A5-273 An organization is planning to deploy an outsourced cloud-based application that is used to track job applicant data for the human resources department. Which of the following should be the **GREATEST** concern to an IS auditor?

A. The service level agreement (SLA) ensures strict limits for uptime and performance.
B. The cloud provider will not agree to an unlimited right-to-audit as part of the SLA.
C. The SLA is not explicit regarding the disaster recovery plan capabilities of the cloud provider.
D. The cloud provider's physical data centers are in multiple cities and countries.

D is the correct answer.

Justification:

A. Although this application may have strict requirements for availability, it is assumed that the service level agreement (SLA) would contain these same elements; therefore, this is not a concern.
B. The right-to-audit clause is good to have, but there are limits on how a cloud service provider may interpret this requirement. The task of reviewing and assessing all the controls in place at a multinational cloud provider would likely be a costly and time-consuming exercise; therefore, such a requirement may be of limited value.
C. Because the SLA would normally specify uptime requirements, the means used to achieve those goals (which would include the specific disaster recovery plan capabilities of the provider) are typically not reviewed in-depth by the customer, nor are they typically specified in a SLA.
D. Having data in multiple countries is the greatest concern because human resources (HR) applicant data could contain personally identifiable information. There may be legal compliance issues if these data are stored in a country with different laws regarding data privacy. While the organization would be bound by the privacy laws where it is based, it may not have legal recourse if a data breach happens in a jurisdiction where the same laws do not apply.

A5-274 An organization is reviewing its contract with a cloud computing provider. For which of the following reasons would the organization want to remove a lock-in clause from the cloud service contract?

A. Availability
B. Portability
C. Agility
D. Scalability

B is the correct answer.

Justification:

A. Removing the customer lock-in clause will not secure availability of the systems resources stored in a cloud computing environment.
B. When drawing up a contract with a cloud service provider, the ideal practice is to remove the customer lock-in clause. It may be important for the client to secure portability of their system assets (i.e., the right to transfer from one vendor to another).
C. Agility refers to efficiency of solutions enabling organizations to respond to business needs faster. This is a desirable quality of cloud computing.
D. Scalability is the strength of cloud computing through the ability to adjust service levels according to changing business circumstances. Therefore, this is not the best option.

A5-275 Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

A. Inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism

C is the correct answer.

Justification:

A. In object-oriented systems an object is called by another module and inherits its data from the calling module. This does not affect security.
B. Dynamic warehousing is not related to the security of object-oriented technology.
C. **Encapsulation is a property of objects, and it prevents accessing either properties or methods that have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.**
D. Polymorphism is the principle of creating different objects that will behave differently depending on the input. This is not a security feature.

A5-276 A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

A. analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
B. WAN capacity is adequate for the maximum traffic demands because saturation has not been reached.
C. the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
D. users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

A is the correct answer.

Justification:

A. **The peak at 96 percent could be the result of a one-off incident (e.g., a user downloading a large amount of data); therefore, analysis to establish whether this is a regular pattern and what causes this behavior should be carried out before expenditure on a larger line capacity is recommended.**
B. A peak traffic load of 96 percent is approaching a critical level, and the auditor should not assume that capacity is adequate at this time or for the foreseeable future. Further investigation is required.
C. If the peak is established to be a regular occurrence without any other opportunities for mitigation (usage of bandwidth reservation protocol or other types of prioritizing network traffic), the line should be replaced because there is the risk of loss of service as the traffic approaches 100 percent. At this point, further research is required.
D. If the peak traffic load is a rare one-off occurrence or if traffic can be reengineered to transfer at other time frames, then user education may be an option. Further investigation will be required.

A5-277 Which of the following **BEST** limits the impact of server failures in a distributed environment?

A. Redundant pathways
B. Clustering
C. Dial backup lines
D. Standby power

B is the correct answer.

Justification:

A. Redundant pathways will minimize the impact of channel communications failures but will not address the problem of server failure.
B. Clustering allows two or more servers to work as a unit so that when one of them fails, the other takes over.
C. Dial backup lines will minimize the impact of channel communications failures but not a server failure.
D. Standby power provides an alternative power source in the event of an energy failure but does not address the problem of a server failure.

A5-278 The **MAIN** reason for requiring that all computer clocks across an organization are synchronized is to:

A. Prevent omission or duplication of transactions.
B. Ensure smooth data transition from client machines to servers.
C. Ensure that email messages have accurate time stamps.
D. Support the incident investigation process.

D is the correct answer.

Justification:

A. The possibility of omission or duplication of transactions will not happen due to lack of clock synchronization.
B. Data transfer has nothing to do with the time stamp.
C. Although the time stamp on an email may not be accurate, this is not a significant issue.
D. During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult, because a time line of events occurring on different systems might not be easily established.

A5-279 When reviewing the configuration of network devices, an IS auditor should **FIRST** identify:

A. The good practices for the type of network devices deployed
B. Whether components of the network are missing
C. The importance of the network devices in the topology
D. Whether subcomponents of the network are being used appropriately

C is the correct answer.

Justification:

A. After understanding the devices in the network, a good practice for using the device should be reviewed to ensure that there are no anomalies within the configuration.
B. Identification of which component is missing can only be known after reviewing and understanding the topology and a good practice for deployment of the device in the network.
C. The first step is to understand the importance and role of the network device within the organization's network topology.
D. Identification of which subcomponent is being used inappropriately can only be known after reviewing and understanding the topology and a good practice for deployment of the device in the network.

A5-280 Which of the following will **BEST** maintain the integrity of a firewall log?

A. Granting access to log information only to administrators
B. Capturing log events in the operating system layer
C. Writing dual logs onto separate storage media
D. Sending log information to a dedicated third-party log server

D is the correct answer.

Justification:

A. To enforce segregation of duties, administrators should not have access to log files. This primarily contributes to the assurance of confidentiality rather than integrity.
B. There are many ways to capture log information—through the application layer, network layer, operating systems layer, etc. However, there is no log integrity advantage in capturing events in the operating systems layer.
C. If it is a highly mission-critical information system, it may be nice to run the system with a dual log mode. Having logs in two different storage devices will primarily contribute to the assurance of the availability of log information, rather than maintaining its integrity.
D. Establishing a dedicated third-party log server and logging events in it is the best procedure for maintaining the integrity of a firewall log. When access control to the log server is adequately maintained, the risk of unauthorized log modification is mitigated, therefore improving the integrity of log information.

A5-281 An IS auditor reviewing a cloud computing environment that is managed by a third party should be **MOST** concerned when:

A. The organization is not permitted to assess the controls in the participating vendor's site.
B. The service level agreement does not address the responsibility of the vendor in the case of a security breach.
C. Laws and regulations are different in the countries of the organization and the vendor.
D. The organization is using an older version of a browser and is vulnerable to certain types of security risk.

B is the correct answer.

Justification:

A. The IS auditor has no role to play if the contract between the parties does not provide for assessment of controls in the other vendor's site.
B. Administration of cloud computing occurs over the Internet and involves more than one participating entity. It is the responsibility of each of the partners in the cloud computing environment to take care of security issues in their own environments. When there is a security breach, the party responsible for the breach should be identified and made accountable. This is not possible if the service level agreement (SLA) does not address the responsibilities of the partners during a security breach.
C. The IS auditor should ensure that the contract addresses the differing laws and regulations in the countries of the organization and the vendor, but having different laws and regulations is not a problem.
D. The IS auditor can make suggestions to the audited entity to use appropriate patches or switch over to safer browsers, and then the IS auditor can follow up on the action taken.

A5-282 Which one of the following can be used to provide automated assurance that proper data files are being used during processing?

A. File header record
B. Version usage
C. Parity checking
D. File security controls

A is the correct answer.

Justification:

A. **A file header record provides assurance that proper data files are being used, and it allows for automatic checking.**
B. Although version usage provides assurance that the correct file and version are being used, it does not allow for automatic checking.
C. Parity checking is a data integrity validation method typically used by a data transfer program. Although parity checking may help to ensure that data and program files are transferred successfully, it does not help to ensure that the proper data or program files are being used.
D. File security controls cannot be used to provide assurance that proper data files are being used and cannot allow for automatic checking.

A5-283 A cyclic redundancy check is commonly used to determine the:

A. Accuracy of data input.
B. Integrity of a downloaded program.
C. Adequacy of encryption.
D. Validity of data transfer.

D is the correct answer.

Justification:

A. Accuracy of data input can be enforced by data validation controls, such as picklists, cross checks, reasonableness checks, control totals and allowed character checks.
B. A checksum or digital signature is commonly used to validate the integrity of a downloaded program or other transferred data.
C. Encryption adequacy is driven by the sensitivity of the data to be protected and algorithms that determine how long it will take to break a specific encryption method.
D. **The accuracy of blocks of data transfers, such as data transfer from hard disks, is validated by a cyclic redundancy check.**

A5-284 An IS auditor is performing a review of a network. Users report that the network is slow and web pages periodically time out. The IS auditor confirms the users' feedback and reports the findings to the network manager. The most appropriate action for the network management team should be to **FIRST:**

A. Use a protocol analyzer to perform network analysis and review error logs of local area network equipment.
B. Take steps to increase the bandwidth of the connection to the Internet.
C. Create a baseline using a protocol analyzer and implement quality of service to ensure that critical business applications work as intended.
D. Implement virtual local area networks to segment the network and ensure performance.

A is the correct answer.

Justification:

A. **In this case, the first step is to identify the problem through review and analysis of network traffic. Using a protocol analyzer and reviewing the log files of the related switches or routers will determine whether there is a configuration issue or hardware malfunction.**
B. Although increasing Internet bandwidth may be required, this may not be needed if the performance issue is due to a different problem or error condition.
C. Although creating a baseline and implementing quality of service will ensure that critical applications have the appropriate bandwidth, in this case, the performance issue may be related to misconfiguration or equipment malfunction.
D. Although implementing virtual local area networks may be good practice for ensuring adequate performance, in this case, the issue may be related to misconfigurations or equipment malfunction.

A5-285 In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

C is the correct answer.

Justification:

A. Logging of changes to production libraries is good practice, but because the administrator can alter the logs, this is not a sufficient control.
B. Although adherence to separation of duties and recruitment of additional staff are preferred , this practice is not always possible in small organizations.
C. **An IS auditor must consider recommending a better process. An IS auditor should recommend a formal change control process that manages and can detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This is a compensating control process.**
D. Requiring a third party to do the changes may not be practical in a small organization where another person with adequate expertise may not be available.

Page intentionally left blank