**Domain 1 - Security+ Cleaned Questions with Answers**

1. **Felicia wants to deploy an encryption solution that will protect files in motion as they are copied between file shares as well as at rest, and also needs it to support granular, per-user security. What type of solution should she select?**A. Partition encryption  
   B. File encryption  
   C. Full-disk encryption  
   D. Record-level encryption **Answer: B.**

Explanation: File encryption meets all of the needs described. Full-disk encryption is easier to deploy and manage but does not protect individual files in motion and does not effectively support multiuser scenarios. Partition-level encryption has the same challenges, albeit at a partition rather than full-disk level. Record-level encryption is typically used in databases to protect individual records or entries.

1. **Valerie wants to use a certificate to handle multiple subdomains for her website, including the sales.example.com and support.example.com subdomains. What type of certificate should she use?**A. A self-signed certificate  
   B. A root of trust certificate  
   C. A CRL certificate  
   D. A wildcard certificate **Answer: D.**

Explanation:Wildcard certificates are used to handle multiple subdomains with a single certificate. A self-signed certificate will not be recognized by browsers and other services, creating confusion for customers. Root of trust certificates and CRL certificates are not types of certificates.

1. **What information is analyzed during a gap analysis?**A. Control objectives and controls intended to meet the objectives  
   B. Physically separate networks and their potential connection points  
   C. Compensating controls and the controls they are replacing  
   D. Security procedures and the policies they are designed to support  
   **Answer: A.**

Explanation: Gap analysis considers control objectives and the controls that are intended to meet the objectives. Physically separate networks, compensating controls, and security procedures may be reviewed, but the primary focus is on control objectives and their corresponding controls.

1. **Susan’s team has recommended an application restart for a production, customer-facing application as part of an urgent patch due to a security update. What technical implication is the most common concern when conducting an application restart?**A. Application configuration changes caused by the restart  
   B. Whether the patch will properly apply  
   C. Lack of security controls during the restart  
   D. The downtime during the restart  
   **Answer: D.**

Explanation: In most production environments downtime is the primary concern when considering an application restart. Many application architectures are designed to allow restarts of individual systems or services without creating an outage or downtime. Configuration changes should not be created by a restart, patches generally apply properly, and security controls should be in place throughout the process.

1. **Using a tool like git is most frequently associated with what critical change management process?**A. Having a backout plan  
   B. Stakeholder analysis  
   C. Version control  
   D. Standard operating procedures (SOPs) **Answer: C.**

Explanation: Organizations frequently use tools like git to build repositories that support their need for version control. Backout plans might note that you need to return to the prior version but will need to include how to do so. Stakeholder analysis and SOPs are not specifically supported by or improved by using git.

1. **Jacob is concerned that the password used for one of his organization’s services is weak, and he wants to make it harder to crack by making it harder to test possible keys during a brute-force attack. What is this technique called?**A. Master keying  
   B. Key stretching  
   C. Key rotation  
   D. Passphrase armoring **Answer: B.**

Explanation:Key stretching makes potentially weak keys more resistant to brute-forcing and often involves using a hash or block cipher repeatedly to make the original value harder to crack. Key rotation is the process of changing keys on a periodic basis to limit the impact of potential exposure. Master keying and passphrase armoring are not commonly used concepts for information security, although master keys are used for physical locks.

1. **Log monitoring is an example of what control category?**A. Managerial  
   B. Operational  
   C. Physical  
   D. Technical **Answer: B.**

Explanation: Operational controls like log monitoring, change management processes, and vulnerability management are all put in place to support managing and using technology in a secure manner. Managerial controls focus **on policies,** physical controls involve tangible measures, and technical controls involve specific technologies.

1. **Rick wants to make offline brute-force attacks against his password file very difficult for attackers. Which of the following is not a common technique to make passwords harder to crack?**A. Use of a salt  
   B. Use of a pepper  
   C. Use of a purpose-built password hashing algorithm  
   D. Encrypting password plain text using symmetric encryption  
   **Answer: D.**

Explanation: Retaining the actual password is not a best practice, and thus encrypting password plain text is not a common technique to make passwords harder to crack. Since the application would need the cryptographic key to read the passwords, anybody who had access to that key could decrypt the passwords. Using a salt, a pepper, and a cryptographic hashing algorithm designed for passwords are all common best practices to prevent offline brute-force attacks.

**9. Diffie-Hellman and RSA are both examples of what important encryption-related solution?**  
A. Rekeying  
B. Certificate revocation protocols  
C. Key exchange algorithms  
D. Key generation algorithms  
**Answer: C. Key exchange algorithms**  
Explanation: Diffie-Hellman and RSA are key exchange algorithms that enable secure key sharing between parties who have not previously communicated, ensuring encrypted communication without prior key exchange.

**10. Sally wants to ensure that her change management process includes a procedure for what to do if the change fails. What should she create to handle this possibility?**  
A. An impact analysis  
B. A backout plan  
C. A regression test  
D. A maintenance window  
**Answer: B. A backout plan**  
Explanation: A backout plan outlines steps to revert a failed change, ensuring systems can be restored to their previous state. Impact analysis assesses potential effects, regression testing checks for reintroduced issues, and maintenance windows are scheduled times for changes.

**11. Theresa is concerned that her scheduled maintenance window may extend beyond the allocated time due to an unexpected issue. What element from the CIA triad is she concerned about?**  
A. Critically  
B. Accessibility  
C. Integrity  
D. Availability  
**Answer: D. Availability**  
Explanation: Extended maintenance windows can disrupt system access, impacting availability, a core element of the CIA triad (confidentiality, integrity, availability). Critically and accessibility are not CIA triad components.

**12. Ann is concerned about vehicles that might impact her organization’s backup generator. What solution should she select to protect a generator installed outside her building near a parking lot?**  
A. A speed bump  
B. An access control vestibule  
C. Bollards  
D. A chain-link fence  
**Answer: C. Bollards**  
Explanation: Bollards are physical barriers designed to prevent vehicle impacts, ideal for protecting infrastructure like generators. Speed bumps slow traffic but don’t prevent impacts, access control vestibules secure entryways, and chain-link fences offer minimal impact resistance.

**13. Ben has deployed a data loss prevention (DLP) tool that inspects data and flags specific data types for review before emails containing it are sent outside the organization. What control type best describes this type of solution?**  
A. Managerial  
B. Detective  
C. Corrective  
D. Preventive  
**Answer: D. Preventive**  
Explanation: DLP tools prevent sensitive data from leaving the organization, making them preventive controls. Managerial controls involve policies, detective controls identify issues after they occur, and corrective controls remediate issues post-event.

**14. What type of control is a policy or procedure?**  
A. Directive  
B. Corrective  
C. Detective  
D. Preventive  
**Answer: A. Directive**  
Explanation: Policies and procedures are directive controls, guiding behavior to achieve security objectives. Corrective controls fix issues, detective controls identify events, and preventive controls stop issues before they occur.

**15. Murati has deployed a file integrity monitoring tool and has configured alerts to notify him if files are modified. What control type best describes this solution?**  
A. Preventive  
B. Deterrent  
C. Directive  
D. Detective  
**Answer: D. Detective**  
Explanation: File integrity monitoring detects unauthorized changes, making it a detective control. Preventive controls stop changes, deterrent controls discourage actions, and directive controls provide guidance.

**16. Charles wants to reduce the threat scope of compromised credentials. What type of the following security controls is best suited to meeting this need?**  
A. Single sign-on  
B. Federation  
C. Zero trust  
D. Multifactor authentication (MFA)  
**Answer: C. Zero trust**  
Explanation: Zero trust continuously verifies all access, minimizing the impact of compromised credentials. MFA enhances authentication but is less comprehensive, while single sign-on and federation may increase risk if credentials are compromised.

**17. Carol wants to obfuscate data that is contained in her database. She wants to be able to refer to the data elements without having the actual data exposed. What type of obfuscation option should she select?**  
A. Tokenization  
B. Encryption  
C. Data masking  
D. Data randomization  
**Answer: A. Tokenization**  
Explanation: Tokenization replaces sensitive data with non-sensitive tokens, allowing reference without exposure. Encryption secures data but requires decryption, data masking hides parts of data, and data randomization is not a standard obfuscation method.

**18. What key is used to decrypt information sent by another individual between two people using public key encryption?**  
A. The recipient’s private key  
B. The recipient’s public key  
C. The sender’s private key  
D. The sender’s public key  
**Answer: A. The recipient’s private key**  
Explanation: In public key encryption, the sender encrypts with the recipient’s public key, and the recipient decrypts with their private key, ensuring only the intended recipient can access the data.

**19. Selah’s organization has recently experienced a breach and the private keys for her organization’s certificates were exposed. What should she immediately do?**  
A. Reissue the certificates with changed hostnames and other details  
B. Replace the certificates with self-signed certificates until they can be replaced by the vendor  
C. Revoke the certificates and place them on a certificate revocation list  
D. Replace the certificates with wildcard certificates  
**Answer: C. Revoke the certificates and place them on a certificate revocation list**  
Explanation: Revoking compromised certificates and adding them to a CRL prevents their misuse. Reissuing with new hostnames is unnecessary, self-signed certificates lack trust, and wildcard certificates don’t address the breach.

**20. Which of the following is not a major concern related to downtime caused by patching and system updates?**  
A. Attackers compromising the system or service while it is offline  
B. Security systems or functions being offline during restart or shutdown processes  
C. Unexpected extended downtime  
D. Dependencies between systems or services related to downtime  
**Answer: A. Attackers compromising the system or service while it is offline**  
Explanation: Offline systems are typically inaccessible to attackers, making this less of a concern. Security systems being offline, extended downtime, and system dependencies are significant issues during patching.

**21. Joanna wants to ensure that the most current version of each component in her application is deployed. What change management process will help the most with this requirement?**  
A. Dependency mapping  
B. Version control  
C. Impact analysis  
D. Allow and deny lists  
**Answer: B. Version control**  
Explanation: Version control tracks and ensures the latest application versions are deployed. Dependency mapping addresses system interactions, impact analysis evaluates change effects, and allow/deny lists manage access.

**22. Greg wants to implement a version control system to ensure that changes are made in ways that will not cause problems for his organization’s critical software. Which of the following is not a common feature of version control systems designed for software source code?**  
A. Atomic operations  
B. File locking  
C. Regression testing  
D. Tagging and labeling  
**Answer: C. Regression testing**  
Explanation: Version control systems support atomic operations, file locking, and tagging/labeling but do not perform regression testing, which is a separate process to ensure new changes don’t reintroduce issues.

**23. Christina wants to implement a physical security control that has the greatest flexibility in how it is applied because she knows that exceptions to security practices may be required at times. Which of the following solutions has the greatest flexibility?**  
A. Video surveillance  
B. Security guards  
C. Access badges  
D. Access control vestibules  
**Answer: B. Security guards**  
Explanation: Security guards offer the most flexibility, as they can adapt to exceptions and make real-time decisions. Video surveillance, access badges, and vestibules are less adaptable to dynamic situations.

**24. Lisa wants to ensure that theft of a device will not lead to exposure of the data contained on the device if the device is locked or turned off. What type of encryption should she select to best ensure this?**  
A. Volume-level encryption  
B. Full-disk encryption  
C. File-level encryption  
D. Partition-level encryption  
**Answer: B. Full-disk encryption**  
Explanation: Full-disk encryption protects all data on a device when locked or off, preventing exposure if stolen. Volume- and partition-level encryption may leave some data unprotected, and file-level encryption is selective.

**25. Mahmoud has been asked to implement an allow list for websites that users at his company can visit. What concern should he bring up to management due to this request?**  
A. Allow lists cannot be used for websites  
B. Allow lists are overly permissive and are likely to allow unwanted sites to be visited  
C. Using an allow list for websites will take a lot of time to maintain  
D. Using an allow list for websites is easily bypassed  
**Answer: C. Using an allow list for websites will take a lot of time to maintain**  
Explanation: Allow lists for websites require ongoing maintenance to ensure all necessary sites are included, which can be time-consuming. They can be configured, are not overly permissive, and bypassing can be mitigated with proper controls.

**26. Which of the following change management processes does not commonly directly involve stakeholders outside of the IT organization?**  
A. Impact analysis  
B. Building the backout plan  
C. The change approval process  
D. Determining the maintenance window  
**Answer: B. Building the backout plan**  
Explanation: Backout plans are typically created by IT staff, focusing on technical steps to revert changes. Impact analysis, change approval, and maintenance window decisions often involve business stakeholders.

**27. What hardware component is used to generate, store, and manage cryptographic keys?**  
A. A CPU  
B. A NSA  
C. A TPM  
D. A CCA  
**Answer: C. A TPM**  
Explanation: A Trusted Platform Module (TPM) is a hardware component for generating, storing, and managing cryptographic keys securely. CPUs are general processors, NSA is not a hardware component, and CCA is a type of cryptographic attack.

**28. Chris wants to check to see if a certificate has been revoked. What protocol can he use to validate the current status of a certificate?**  
A. TLS  
B. OCRS  
C. SSL  
D. OCSP  
**Answer: D. OCSP**  
Explanation: The Online Certificate Status Protocol (OCSP) checks certificate revocation status in real time. TLS and SSL are encryption protocols, and OCRS is not a valid protocol.

**29. Brian’s organization uses a process where a secure module boots systems, then monitors them as each boot stage proceeds. It validates each signed boot stage and reports on whether the boot process was correct or not when complete. What is the secure module used to verify these stages called?**  
A. A secure initiation manager  
B. A root of trust  
C. A boot hash  
D. A cryptographic boot manager  
**Answer: B. A root of trust**  
Explanation: A root of trust is a secure module that validates signed boot stages, ensuring a trusted boot process. Other options are not standard terms for this function.

**30. A vulnerability scan shows that an embedded device that Alice is responsible for has a vulnerability. She knows the vendor is no longer in business and that there is no updated firmware or software update for the device. To resolve the issue, Alice places a firewall between the device and the rest of the network and creates rules that prevent the vulnerable service from being available to other devices. What type of control has Alice deployed?**  
A. A directive control  
B. A compensating control  
C. A detective control  
D. A procedural control  
**Answer: B. A compensating control**  
Explanation: A compensating control mitigates risks when primary controls (e.g., patching) are unavailable, as with Alice’s firewall rules. Directive controls are policies, detective controls identify issues, and procedural controls are not a Security+ category.

**31. Jason knows that his Apple system uses a separate portion of its SoC (system on chip) to store keys and biometric information. What is this specialized component called?**  
A. A TPM  
B. A HSM  
C. A secure enclave  
D. A screened subnet  
**Answer: C. A secure enclave**  
Explanation: Apple’s secure enclave is a dedicated SoC component for storing keys and biometric data securely. TPMs and HSMs serve similar functions but are distinct, and a screened subnet is a network security concept.

**32. What change management term is used to describe the processes that an organization uses for each change that is made to ensure that a consistent process is used?**  
A. Standard operating procedures  
B. A change plan  
C. Fixed operating procedures  
D. A backout plan  
**Answer: A. Standard operating procedures**  
Explanation: Standard operating procedures (SOPs) define consistent processes for changes. Change plans are specific to individual changes, backout plans address reversions, and fixed operating procedures is not a standard term.

**33. Jack knows that there are three common types of database encryption. Which of the following is not a common type of database encryption?**  
A. Sensitivity-based encryption  
B. Transparent data encryption  
C. Field-level encryption  
D. Column-level encryption  
**Answer: A. Sensitivity-based encryption**  
Explanation: Transparent data encryption, field-level, and column-level encryption are standard database encryption types. Sensitivity-based encryption is not a recognized term in this context.

**34. Ujamas wants to conduct a gap analysis as part of his security efforts. Which of the following best describes what he will analyze?**  
A. Which services are not configured properly  
B. Whether current patches are installed on all systems  
C. The security program as implemented versus best practices  
D. Legal requirements versus the security program  
**Answer: C. The security program as implemented versus best practices**  
Explanation: Gap analysis compares an organization’s security program against best practices (e.g., NIST, ISO) to identify deficiencies. Other options are too narrow to encompass the full scope of gap analysis.

**35. Brandon wants to deploy a detective control that will help him with physical security threats. Which of the following fits his needs?**  
A. Fencing  
B. Lighting  
C. Video surveillance  
D. Bollards  
**Answer: C. Video surveillance**  
Explanation: Video surveillance detects physical security incidents after they occur, making it a detective control. Fencing, lighting, and bollards are preventive controls.

**36. Jack has deployed a system that appears to attackers to be a vulnerable system. The system is specifically designed to capture information and data from attacks to allow for later analysis. What type of tool has Jack deployed?**  
A. A tarpit  
B. A honeypot  
C. A beehive  
D. An intrusion detection system  
**Answer: B. A honeypot**  
Explanation: Honeypots are decoy systems designed to attract and analyze attacker behavior. Tarpits slow attackers, beehives is not a term, and IDSs detect but don’t mimic vulnerable systems.

**37. Renee wants to ensure that her logs support nonrepudiation. What should she do to ensure this?**  
A. Encrypt, then hash the logs  
B. Hash the logs and then digitally sign them  
C. Digitally sign the log file, then encrypt it  
D. Hash, then encrypt the logs  
**Answer: B. Hash the logs and then digitally sign them**  
Explanation: Hashing logs ensures integrity, and digitally signing the hash ensures nonrepudiation by proving the log’s origin. Encryption alone doesn’t provide nonrepudiation, and other options are less effective.

**38. Isaac wants to deploy sensors to detect intruders in a facility, but he is concerned about the sensors being overly sensitive. What type of sensor is best suited to detecting intruders in an open office environment without significant expense or issues with sensitivity?**  
A. Infrared  
B. Pressure  
C. Microwave  
D. Ultrasonic  
**Answer: A. Infrared**  
Explanation: Infrared sensors are cost-effective and reliable for detecting intruders in open spaces without excessive sensitivity. Pressure sensors are specialized, microwave sensors may penetrate walls, and ultrasonic sensors are less common.

**39. Wayne wants to allow systems to claim identities as part of his AAA process. Which of the following is most commonly used to identify both individuals and systems?**  
A. Tokens  
B. Smartcards  
C. Certificates  
D. Usernames  
**Answer: C. Certificates**  
Explanation: Certificates are widely used to identify both systems and individuals in AAA processes, providing strong authentication. Tokens and smartcards are user-focused, and usernames are less secure for systems.

**40. What are considerations like database and network connectivity, authentication system access, and network time availability considered in the context of change management processes?**  
A. Allowed services  
B. Standard operating procedures  
C. Denied services  
D. Dependencies  
**Answer: D. Dependencies**  
Explanation: Database connectivity, authentication, and network time are dependencies that must be available for successful changes. SOPs define processes, and allowed/denied services relate to access control.

**41. What role does the policy engine play in a zero-trust environment?**  
A. It creates new administrative policies based on user behavior  
B. It grants access based on policies created by administrators and based on security systems data  
C. It enforces policies by monitoring connections between clients and servers  
D. It suggests new administrative policies based on usage patterns for adoption by the organization  
**Answer: B. It grants access based on policies created by administrators and based on security systems data**  
Explanation: The policy engine evaluates policies and security data to grant access in zero-trust environments. Enforcement occurs at policy enforcement points, and policy creation/suggestion is not its role.

**42. Which of the following is not a common post-change activity found in change management practices?**  
A. Updating diagrams  
B. Updating procedures  
C. Updating policies  
D. Updating contracts  
**Answer: D. Updating contracts**  
Explanation: Contracts are updated during renewals, not as a routine post-change activity. Diagrams, procedures, and policies are commonly updated to reflect technical changes.

**43. Which of the following activities should Alaina not restrict as part of her preparation for a change window?**  
A. Patching  
B. Scaling clustered systems up or down  
C. Changing hostnames  
D. Modifying database configurations  
**Answer: B. Scaling clustered systems up or down**  
Explanation: Scaling clustered systems doesn’t typically alter system configurations, making it safe during change windows. Patching, hostname changes, and database modifications can introduce risks and should be restricted.

**44. What two key features define blockchain ledgers?**  
A. They are immutable and nontransferable  
B. They are shared and can be modified by a vote among all participants  
C. They are unique to each participant and are atomic  
D. They are shared and immutable  
**Answer: D. They are shared and immutable**  
Explanation: Blockchain ledgers are shared across participants and immutable, meaning records cannot be altered once written. Other options misrepresent blockchain characteristics.

**45. Damian issues the following command on his Linux server: openssl req -new -newkey rsa:2048 -nodes -keyout exampleserver.key -out exampleserver.csr. What has he done?**  
A. Created a certificate signing request  
B. Created a certificate revocation request  
C. Signed a certificate signing request  
D. Updated the OCSP record for a certificate  
**Answer: A. Created a certificate signing request**  
Explanation: The command generates a certificate signing request (CSR) and private key for submission to a CA. It does not revoke, sign, or update OCSP records.

**46. Nick’s organization sets aside Saturday nights from 2 a.m. to 4 a.m. for scheduled maintenance. What is this type of reserved time typically called?**  
A. Allocated downtime  
B. A maintenance window  
C. An unscheduled outage  
D. An allowed outage  
**Answer: B. A maintenance window**  
Explanation: A maintenance window is a preplanned time for maintenance activities, minimizing disruption. Unscheduled outages are unplanned, and other terms are not standard.

**47. Megan wants to assess the impact of a change as part of her change management process. Which of the following is most likely to help her assess impact?**  
A. A backout plan  
B. An estimate of the downtime expected  
C. A list of stakeholders  
D. A list of dependencies for impacted systems  
**Answer: B. An estimate of the downtime expected**  
Explanation: Estimating downtime helps assess the business impact of a change. Backout plans address failures, stakeholders aid communication, and dependencies ensure technical success but don’t directly assess impact.

**48. Jared wants to estimate the downtime that will result as part of a planned change. Which of the following methods will most effectively help him estimate downtime?**  
A. Average the downtime from other recent changes  
B. Contact the vendor for time estimates for the change  
C. Perform the change in a test environment  
D. Use a fixed maintenance window  
**Answer: C. Perform the change in a test environment**  
Explanation: Testing in a controlled environment provides accurate downtime estimates. Averages are unreliable, vendors lack context, and fixed windows don’t estimate duration.

**49. An encryption method in which all participants have the same key is known as which of the following types of encryption?**  
A. Shared hashing  
B. Asymmetric encryption  
C. Symmetric encryption  
D. Universal encryption  
**Answer: C. Symmetric encryption**  
Explanation: Symmetric encryption uses a single shared key for encryption and decryption. Asymmetric encryption uses key pairs, and shared hashing and universal encryption are not valid terms.

**50. What important encryption challenge does asymmetric encryption help with by using public keys?**  
A. Evil twins  
B. Collision resistance  
C. Key length  
D. Key exchange  
**Answer: D. Key exchange**  
Explanation: Asymmetric encryption enables secure key exchange by using public keys, solving the challenge of sharing keys securely. Evil twins, collision resistance, and key length are unrelated.

**51. Ricky’s cloud provider offers a dedicated hardware security module. Which of the following capabilities is it unlikely to offer?**  
A. Validating secure boot processes  
B. Key generation  
C. Encrypting and decrypting data  
D. Creating digital signatures  
**Answer: A. Validating secure boot processes**  
Explanation: Hardware security modules (HSMs) handle key generation, encryption/decryption, and digital signatures but not secure boot validation, which is typically a TPM function.

**52. Michelle believes that an image she has discovered in an attacker’s directory of files contains additional information that has been hidden in it. What is this type of obfuscation called?**  
A. Steganography  
B. Image hashing  
C. PNG warping  
D. Image blocking  
**Answer: A. Steganography**  
Explanation: Steganography hides data within images or other files. Image hashing, PNG warping, and image blocking are not standard obfuscation techniques.

**53. Which of the following is not a common transport encryption protocol?**  
A. TLS  
B. IPSec  
C. SAML  
D. SSH  
**Answer: C. SAML**  
Explanation: SAML is used for authentication and authorization, not transport encryption. TLS, IPSec, and SSH are standard protocols for securing data in transit.

**54. What technology is record-level encryption most commonly associated with?**  
A. Stored audio files  
B. Databases  
C. Physical disks  
D. Removable storage  
**Answer: B. Databases**  
Explanation: Record-level encryption is commonly used in databases to secure individual records with unique keys, enhancing data privacy.

**55. Yasmine submits the Windows BitLocker key to a central repository after she encrypts the machine. The central repository allows files to be uploaded, but not read, and is protected with access requiring special permissions. What type of solution is Yasmine’s company using?**  
A. A hardware security module  
B. Perfect forward secrecy  
C. Key escrow  
D. Private keys  
**Answer: C. Key escrow**  
Explanation: Key escrow stores encryption keys securely for authorized access, as described. HSMs manage keys, perfect forward secrecy changes keys frequently, and private keys are part of encryption, not the solution.

**56. Valerie wants to authenticate her systems using her AAA system. Which of the following options is best suited to system authentication?**  
A. Asymmetric authentication  
B. Certificate-based authentication  
C. Symmetric authentication  
D. PIN-based authentication  
**Answer: B. Certificate-based authentication**  
Explanation: Certificate-based authentication is ideal for system authentication in AAA, providing strong, scalable security. Asymmetric and symmetric are encryption types, and PINs are user-focused.

**57. Valentine wants to detect if an intruder has accessed a secured file server. Which of the following techniques will work best with a data loss prevention tool to identify data exfiltration?**  
A. A honeypot  
B. A honeynet  
C. A honeyfile  
D. A honeytoken  
**Answer: C. A honeyfile**  
Explanation: Honeyfiles are decoy files monitored by DLP tools to detect exfiltration. Honeypots and honeynets are systems or networks, and honeytokens are credentials, not files.

**58. Jason has recommended that additional lighting be put in place on the exterior of his building as part of a security upgrade. What type of control is lighting?**  
A. Operational  
B. Deterrent  
C. Corrective  
D. Technical  
**Answer: B. Deterrent**  
Explanation: Lighting deters potential intruders by increasing visibility, making it a deterrent control. It’s also a physical control, not operational, corrective, or technical.

**59. Which of the following controls is typically the most expensive to implement?**  
A. Bollards  
B. Access control vestibules  
C. Security guards  
D. Access badges  
**Answer: C. Security guards**  
Explanation: Security guards require ongoing human resources, making them the most expensive. Bollards, vestibules, and badges have lower recurring costs.

**60. Frankie wants to validate the integrity of a file by comparing it against an original copy. Which of the following solutions both fulfills this requirement and avoids known security issues?**  
A. Hash the original file and the current file using MD5 and compare the hashes  
B. Hash the original file and the current file using SHA-1 and compare the hashes  
C. Hash the original file and the current file using SHA-256 and compare the hashes  
D. Hash the original file and the current file using AES and compare the hashes  
**Answer: C. Hash the original file and the current file using SHA-256 and compare the hashes**  
Explanation: SHA-256 is a secure hashing algorithm for verifying file integrity. MD5 and SHA-1 have known vulnerabilities, and AES is an encryption algorithm, not a hashing method.

**61. Joanna’s organization has a policy that requires a user’s password to be immediately reset to lock accounts if the account is determined to have been successfully phished. What type of control is this?**  
A. A detective control  
B. A directive control  
C. A compensating control  
D. A corrective control  
**Answer: B. A directive control**  
Explanation: The policy directing password resets is a directive control, guiding actions post-phishing. The reset itself is corrective, but the policy is directive.

**62. Jackie wants to implement an AAA system for her network. What AAA protocol is commonly used for network devices?**  
A. OpenID  
B. SAML  
C. RADIUS  
D. TANGENT  
**Answer: C. RADIUS**  
Explanation: RADIUS is widely used for AAA on network devices. OpenID and SAML are for federated identity, and TANGENT is not a protocol.

**63. Scott wants to automate policy creation in his zero-trust environment’s policy engine. Which of the following is not a typical component for automated data and event-driven policy management?**  
A. A SIEM  
B. Threat feeds  
C. Infrared sensor data  
D. EDR tools  
**Answer: C. Infrared sensor data**  
Explanation: SIEM, threat feeds, and EDR tools provide data for zero-trust policy automation. Infrared sensor data is physical security-related, not typically used in zero-trust policy engines.

**64. Valerie’s organization has deployed a zero-trust solution, and Valerie receives an authentication prompt when she is attempting to access a file server. What component of the zero-trust architecture is she interacting with?**  
A. A policy enforcement point  
B. A policy administrator  
C. The policy engine  
D. The trust manager  
**Answer: A. A policy enforcement point**  
Explanation: Policy enforcement points (PEPs) handle authentication and authorization prompts in zero-trust, interfacing with the policy engine. Other options are not standard zero-trust components.

**65. Matt is assessing his organization’s zero-trust model against the NIST Zero Trust Maturity Model. Which of the following is not a common element of zero-trust systems that would be assessed as part of the model?**  
A. Identity  
B. Business model  
C. Networks  
D. Devices  
**Answer: B. Business model**  
Explanation: NIST’s Zero Trust Maturity Model assesses identity, devices, networks, applications, and data. Business model is not a security-focused element in this context.

**66. Quentin wants to deploy a single sign-on system to allow his users to log in to cloud services. Which of the following technologies is he most likely to deploy?**  
A. OpenID  
B. Kerberos  
C. LDAP  
D. TACACS+  
**Answer: A. OpenID**  
Explanation: OpenID is commonly used for single sign-on to cloud services. Kerberos and LDAP are typically on-premises, and TACACS+ is for network device authentication.

**67. Marty wants to deploy a corrective control to deal with a recently compromised system. Which of the following would be considered a corrective control?**  
A. Patching the vulnerability that allowed the compromise to occur  
B. Deploying full-disk encryption  
C. Deploying an endpoint detection and response (EDR) tool  
D. Enabling logging and sending logs to a SIEM  
**Answer: A. Patching the vulnerability that allowed the compromise to occur**  
Explanation: Patching fixes a specific vulnerability post-compromise, making it corrective. Encryption and EDR are preventive, and logging is detective.

**68. What important encryption feature is not supported by symmetric encryption?**  
A. Confidentiality  
B. Integrity  
C. Nonrepudiation  
D. Authentication  
**Answer: C. Nonrepudiation**  
Explanation: Symmetric encryption uses a shared key, lacking nonrepudiation, which requires proving the sender’s identity (achieved via asymmetric encryption). It supports confidentiality, integrity, and authentication.

**69. Theresa wants to use a cloud-hosted security solution that will allow her to safely store and manage secrets. What type of solution should she select?**  
A. A TPM  
B. A CA  
C. A KMS  
D. A CSR  
**Answer: C. A KMS**  
Explanation: A Key Management System (KMS) securely stores and manages secrets like keys and certificates in the cloud. TPMs are hardware-based, CAs issue certificates, and CSRs are requests.

**70. Joanna is reviewing her account information on an e-commerce website and sees her credit card number displayed as XXXX-XXXX-XXXX-1234. What type of data obfuscation is in use?**  
A. Hashing  
B. Data masking  
C. Field encryption  
D. Tokenization  
**Answer: B. Data masking**  
Explanation: Data masking obscures parts of sensitive data (e.g., credit card numbers) while displaying some digits. Hashing is one-way, encryption secures entire fields, and tokenization replaces data with tokens.

**71. Amanda’s organization wants to use a decentralized blockchain to store data. Which of the following is true about a decentralized blockchain?**  
A. No individual or group controls the blockchain  
B. Only cryptocurrency-related data can be stored in a blockchain  
C. Blockchain data can be changed after being stored by the original submitter  
D. Blockchain ledgers are stored on central servers chosen by regular elections among blockchain participants  
**Answer: A. No individual or group controls the blockchain**  
Explanation: Decentralized blockchains are controlled by no single entity, relying on distributed consensus. They store various data types, are immutable, and are maintained by participants, not central servers.

**72. What role does a subordinate CA have in a CA hierarchy?**  
A. Subordinate CAs issue certificates based on subdomains  
B. Subordinate CAs provide control over certificate issuance while avoiding the cost of being a root CA  
C. Subordinate CAs validate root CA activities to ensure auditability  
D. Subordinate CAs review certificate signing requests before forwarding them to the root CA  
**Answer: B. Subordinate CAs provide control over certificate issuance while avoiding the cost of being a root CA**  
Explanation: Subordinate CAs issue certificates under a root CA, reducing costs and complexity while maintaining control. They don’t limit to subdomains, validate root CAs, or merely review CSRs.

**73. Which of the following sensor types is commonly used to detect footsteps?**  
A. Infrared  
B. Pressure  
C. Microwave  
D. Ultrasonic  
**Answer: B. Pressure**  
Explanation: Pressure sensors detect footsteps by sensing weight changes. Infrared and microwave sensors detect motion, and ultrasonic sensors are less common for this purpose.

**74. Which of the following is not a managerial control?**  
A. Risk assessments  
B. Including security in change management processes  
C. Security planning exercises  
D. Implementing firewalls  
**Answer: D. Implementing firewalls**  
Explanation: Firewalls are technical controls. Managerial controls, like risk assessments, security in change management, and planning exercises, focus on risk management processes.

**75. What purpose do third-party certificates serve for customers of cloud services?**  
A. They reduce costs by using bring-your-own certificates  
B. They allow certificates for domains other than the service provider’s domain  
C. They provide control over cryptographic security for the customer  
D. They allow more flexibility in TLS version selection  
**Answer: C. They provide control over cryptographic security for the customer**  
Explanation: Third-party certificates give customers control over private keys and CSRs, enhancing security. Costs may not decrease, domains are supported by providers, and TLS versions are not the primary benefit.

**76. Which of the following is not a common control focused on availability?**  
A. Uninterruptible power systems  
B. Redundant internet connectivity  
C. Disk encryption  
D. Load balancers  
**Answer: C. Disk encryption**  
Explanation: Disk encryption ensures confidentiality, not availability. UPS, redundant connectivity, and load balancers support system uptime and availability.

**77. What term describes a collection of honeypots on a network intended to capture information about cybersecurity threats?**  
A. A honeyfarm  
B. A honeynet  
C. A honeycluster  
D. A darknet  
**Answer: B. A honeynet**  
Explanation: A honeynet is a network of honeypots designed to capture threat data. Honeyfarm and honeycluster are not standard terms, and darknets monitor unused network space.

**78. Skip wants to implement a deterrent control to prevent physical security issues for his organization. Which of the following controls should he select?**  
A. A fence  
B. A generator  
C. Access badges  
D. A camera system  
**Answer: A. A fence**  
Explanation: Fences deter unauthorized access by creating a physical barrier. Generators ensure availability, badges are technical/preventive, and cameras are detective.

**79. What holds the position of the root of trust in a certificate chain?**  
A. A hardened hardware device  
B. A TPM  
C. The root certificate  
D. A wildcard certificate  
**Answer: C. The root certificate**  
Explanation: The root certificate is the root of trust in a certificate chain, anchoring the trust hierarchy. Hardware devices and TPMs may store it, and wildcard certificates are not roots.

**80. Jill needs to explain the concept of open public ledgers to her organization as management wants to adopt a blockchain-based system. What should she tell them about access to the ledger?**  
A. Members must be added by a vote of all current members  
B. Anyone can join at any time  
C. Members must be added by a vote of more than 51 percent of current members  
D. Ledgers are public but membership is private and controlled by the creator of the ledger  
**Answer: B. Anyone can join at any time**  
Explanation: Open public ledgers allow anyone to join and access the blockchain without restrictions, a key feature of public blockchains.

**81. Olivia wants to use a self-signed certificate in her test environment for her organization’s services to save money on commercial certificates. What warning should her team give her about the use of self-signed certificates in a test environment?**  
A. Certificate root of trust validation attempts will fail if implemented  
B. Self-signed certificates cannot be used for external users to support SSL  
C. Self-signed certificates cannot be used for internal users to support SSL  
D. Browsers will not allow self-signed certificates to be used when browsing sites  
**Answer: A. Certificate root of trust validation attempts will fail if implemented**  
Explanation: Self-signed certificates lack a trusted CA, causing validation failures in software expecting trusted roots, which can disrupt testing. They can support SSL internally/externally but trigger browser warnings.

**82. Amanda is concerned about issues with dependencies that may be found during her pending change. What practice should she implement to help ensure unexpected dependency issues are not encountered?**  
A. Update organizational policies and procedures before the change  
B. Update functional diagrams before the change  
C. Validate the change in a test environment  
D. Document legacy applications that may create dependencies  
**Answer: C. Validate the change in a test environment**  
Explanation: Testing changes in a controlled environment identifies dependency issues before production deployment. Updating policies/diagrams or documenting legacy apps is less effective for catching unexpected issues.

**83. Lucca has implemented an authentication scheme that relies on ticket-granting tickets as part of the authentication process. What common authentication service has he implemented?**  
A. TACACS+  
B. Kerberos  
C. MS-CHAP  
D. EAP  
**Answer: B. Kerberos**  
Explanation: Kerberos uses ticket-granting tickets for secure authentication. TACACS+ is for network devices, MS-CHAP is for VPNs, and EAP is for wireless authentication.

**84. Jocelyn wants to select a modern encryption algorithm for use in her organization. Which of the following is a currently recommended encryption algorithm?**  
A. AES-256  
B. SHA1  
C. DES  
D. Blowfish  
**Answer: A. AES-256**  
Explanation: AES-256 is a modern, secure encryption algorithm. SHA1 is a hashing algorithm, DES is outdated, and Blowfish is less preferred for new implementations.

**85. Elizabeth wants to classify the following controls by their category: What category best describes lighting, fences, bollards, and access control vestibules?**  
A. Technical  
B. Managerial  
C. Operational  
D. Physical  
**Answer: D. Physical**  
Explanation: Lighting, fences, bollards, and vestibules are physical controls, impacting the physical environment to enhance security.

**86. Jack wants to ensure the integrity of a file that he is sending to a third party via email. How can he provide the integrity of a file to an organization that he has not done business with before?**  
A. Encrypt the file and send it to them  
B. Digitally sign the file  
C. Send a hash of the file in a separate email  
D. Email the file size and original name in a separate email  
**Answer: B. Digitally sign the file**  
Explanation: Digital signatures ensure file integrity and authenticity, verifiable with Jack’s public key. Encryption protects confidentiality, separate hashes lack nonrepudiation, and file size/name don’t ensure integrity.

**87. Annie notices that her browser shows that the certificate for the site she is visiting is not valid. After performing some checks, she sees that the certificate is on the CA’s certificate revocation list. Which of the following is not a reason for a certificate to be on a CRL?**  
A. The CA is compromised  
B. The certificate’s private key was compromised  
C. The certificate was signed with a stolen key  
D. The certificate expired  
**Answer: D. The certificate expired**  
Explanation: Expired certificates are not typically added to CRLs, as expiration is handled by validity dates. Compromised CAs, private keys, or stolen keys justify revocation.

**88. Mohinder wants to use modern, secure hashing algorithms to validate files against known good originals. Which of the following hashing algorithms should he select?**  
A. MD5  
B. SHA-1  
C. AES-256  
D. SHA-256  
**Answer: D. SHA-256**  
Explanation: SHA-256 is a secure, modern hashing algorithm. MD5 and SHA-1 have vulnerabilities, and AES-256 is for encryption, not hashing.

**89. Derrick wants to validate an encrypted and digitally signed message sent using asymmetric encryption. What does he need from the sender to validate the message?**  
A. The sender’s private key  
B. Derrick’s private key  
C. The sender’s public key  
D. Derrick’s public key  
**Answer: C. The sender’s public key**  
Explanation: The sender’s public key verifies the digital signature, ensuring the message’s authenticity and integrity. Private keys are not shared, and Derrick’s keys are for his own messages.

**90. The major patch release that Susan’s team installed has failed, resulting in a nonworking service. What should her team do according to change management best practices?**  
A. Declare an outage  
B. Follow the documented backout plan  
C. Restore from backups to the previous version  
D. Uninstall the patch and validate service function  
**Answer: B. Follow the documented backout plan**  
Explanation: Following the backout plan ensures a structured reversal of the failed change. Declaring an outage, restoring backups, or uninstalling may be steps, but the plan guides the process.

**91. The web server that Angela’s organization manages was recently compromised and the SSL certificate’s private key was accessed by attackers. Angela’s team has completed remediation and has created a new CSR, including a new private key that they have secured. What type of control type best describes the creation of a new key and certificate in this circumstance?**  
A. Corrective  
B. Compensating  
C. Deterrent  
D. Detective  
**Answer: A. Corrective**  
Explanation: Creating a new key and certificate post-compromise corrects the security issue, making it a corrective control. Compensating controls address policy exceptions, deterrents prevent attacks, and detectives identify issues.

**92. Mikayla’s zero-trust system has received a request for access with an identity, and the basic criteria for access have been met. What should the system do next before providing access to the resource requested?**  
A. Check the remote system’s security status  
B. Require reauthentication using MFA  
C. Check the user’s rights to ensure they can access the resource  
D. Determine its level of confidence in the request  
**Answer: C. Check the user’s rights to ensure they can access the resource**  
Explanation: After identity verification, zero-trust systems check authorization (user rights) to ensure access is permitted. Security status and confidence levels are part of broader checks, and MFA may not be required again.

**93. Charles sets up an RDP server on an isolated network segment and places a file on it called passwords.xlsx. He then configures his IPS and DLP systems to monitor for that file exiting the network segment. What type of tool has Charles deployed?**  
A. A honeyfile  
B. A SQL trap  
C. A red flag  
D. A trigger file  
**Answer: A. A honeyfile**  
Explanation: A honeyfile is a decoy file designed to detect unauthorized access or exfiltration, as Charles has implemented. Other options are not standard terms.

**94. Lucca is using precomputed rainbow tables to attempt to crack hashed passwords from a data breach. He knows that two users have the same password, but the hashes do not match. What password hash security technique has Lucca most likely encountered?**  
A. Password encryption  
B. Salting  
C. Key stretching  
D. Password mismatching  
**Answer: B. Salting**  
Explanation: Salting adds unique random data to passwords before hashing, ensuring identical passwords produce different hashes, thwarting rainbow table attacks. Encryption, key stretching, and mismatching are not the issue here.

**95. What operating system is commonly associated with secure enclaves?**  
A. Windows  
B. iOS  
C. Linux  
D. Android  
**Answer: B. iOS**  
Explanation: iOS uses secure enclaves in Apple devices to store sensitive data like keys and biometrics. Other OSs may use similar technologies but are less associated with secure enclaves.

**96. Isaac is concerned that the passwords that his users are creating are too short and can be easily brute-forced if their hashes were compromised. Rather than make his users remember longer passwords, he would like to implement a technical solution to help make the hashes more resistant to cracking. What solution can he use to help with this?**  
A. Implement pass-the-hash algorithms  
B. Use a collision-resistant hashing algorithm  
C. Implement key stretching techniques  
D. Encrypt passwords rather than hashing them  
**Answer: C. Implement key stretching techniques**  
Explanation: Key stretching (e.g., PBKDF2) increases the computational effort needed to crack hashes, strengthening short passwords. Pass-the-hash is an attack, collision resistance is standard, and encrypting passwords is insecure.

**97. Christina wants to implement access badges printed with picture IDs for her organization, but she wants to use a wireless reader. What access badge technology is commonly implemented in scenarios like this?**  
A. Wi-Fi-enabled access badges  
B. RFID access badges  
C. Bluetooth-enabled access badges  
D. NFC access badges  
**Answer: B. RFID access badges**  
Explanation: RFID badges are commonly used for wireless access control, balancing security and convenience. Wi-Fi and Bluetooth are less practical, and NFC is emerging but less common.

**98. Kendra’s vulnerability management team has discovered that Internet of Things (IoT) devices deployed a few years ago to monitor temperatures for critical refrigerated equipment are vulnerable to a new attack. After reviewing the issue, her team has discovered that the devices are no longer supported and that the manufacturer has gone out of business. They suggest moving the devices to an isolated network to help protect them. What type of control has Kendra’s team suggested?**  
A. A corrective control  
B. A compensating control  
C. A confidentiality control  
D. A coordinated control  
**Answer: B. A compensating control**  
Explanation: Isolating unpatchable devices mitigates risk when primary controls are unavailable, making it a compensating control. Corrective controls fix issues post-event, and confidentiality/coordinated controls are not Security+ categories.

**99. Which of the following is not a common factor in adaptive authentication for zero trust?**  
A. Where the user is logging in from  
B. Whether the user has logged in recently from another device  
C. What device the user is logging in from  
D. If the device is configured correctly  
**Answer: B. Whether the user has logged in recently from another device**  
Explanation: Adaptive authentication considers location, device type, and configuration but not recent logins from other devices unless they raise specific risks (e.g., geographic anomalies).

**100. Juan’s organization is designing their zero-trust model. Which of the following statements is true for network security zones?**  
A. All communication is secured, regardless of the network security zone it occurs in  
B. Communication receives additional security in low-trust zones  
C. Communication receives less security in high-trust zones  
D. All zero-trust networks are considered secured zones  
**Answer: A. All communication is secured, regardless of the network security zone it occurs in**  
Explanation: Zero-trust requires all communication to be secured, regardless of zone, eliminating trust assumptions. Other options contradict zero-trust principles.

**101. What advantage do microwave sensors have over infrared sensors?**  
A. They can detect heat signatures  
B. They are cheaper than infrared sensors  
C. They can penetrate some types of walls  
D. They do not interfere with sensitive equipment  
**Answer: C. They can penetrate some types of walls**  
Explanation: Microwave sensors can penetrate walls, offering broader coverage than infrared, which is limited to line-of-sight. They don’t detect heat, aren’t cheaper, and may interfere with equipment.

**102. Isaac is conducting a physical penetration test and wants to bypass an access control vestibule. What must he accomplish?**  
A. He needs to persuade an individual to allow him to follow them through a single door  
B. He needs to acquire an individual’s access card  
C. He needs to persuade an individual to allow him to follow them through two doors in a row  
D. He needs to acquire the individual’s access PIN  
**Answer: C. He needs to persuade an individual to allow him to follow them through two doors in a row**  
Explanation: Access control vestibules require passing through two secured doors, so tailgating both is necessary. A single door or stolen credentials alone won’t bypass the vestibule.

**103. Rachel wants to select an obfuscation method that will allow her customer service representatives to validate customer identities without providing full access to customer data. What should she select?**  
A. Tokenization  
B. Data masking  
C. Steganography  
D. Hashing  
**Answer: B. Data masking**  
Explanation: Data masking reveals partial data (e.g., last four digits of a card) for validation without full exposure. Tokenization replaces data, steganography hides data, and hashing is one-way.

**104. Valerie’s manager has informed her that version control must be implemented for her development team’s work. Which of the following is not a common, security-related reason for version control?**  
A. To help with patching  
B. To track each contributor’s workload  
C. To ensure the proper version is deployed  
D. To help with change management  
**Answer: B. To track each contributor’s workload**  
Explanation: Version control supports patching, correct version deployment, and change management but not workload tracking, which is a project management function.

**105. Jackie’s change management process involves reporting functional validation test results to stakeholders. Which of the following is not a common stakeholder or stakeholder group for an application upgrade?**  
A. Application administrators  
B. Service owners  
C. System administrators  
D. Auditors  
**Answer: D. Auditors**  
Explanation: Application admins, service owners, and system admins are typical stakeholders for upgrade validation. Auditors are involved in compliance, not routine upgrades.

**106. How many keypairs are required for four individuals to communicate securely using asymmetric encryption?**  
A. 1  
B. 4  
C. 8  
D. 12  
**Answer: B. 4**  
Explanation: Each individual requires one keypair (public and private) for asymmetric encryption, so four individuals need four keypairs.

**107. Michelle wants to store secrets for her organization in a cloud service. She wants to ensure the greatest level of security for her organization, and she is willing to spend more money to provide that security. What solution should she look for?**  
A. A shared cloud TPM  
B. A shared cloud HSM  
C. A dedicated hardware cloud TPM  
D. A dedicated hardware cloud HSM  
**Answer: D. A dedicated hardware cloud HSM**  
Explanation: A dedicated hardware cloud HSM offers the highest security for storing secrets, avoiding shared hardware risks. TPMs are for secure boot, not cloud secret storage.

**108. Murali wants to digitally sign a file. What key does he need to sign it?**  
A. The recipient’s private key  
B. His private key  
C. The recipient’s public key  
D. His public key  
**Answer: B. His private key**  
Explanation: Murali signs with his private key, allowing recipients to verify with his public key, ensuring authenticity and integrity.

**109. What information is necessary for a certificate to be identified properly in an OCSP request?**  
A. The domain name  
B. The original requestor’s name  
C. The certificate’s serial number  
D. The identifier for the open public ledger entry  
**Answer: C. The certificate’s serial number**  
Explanation: OCSP requests use the certificate’s serial number to check its status. Domain names, requestor names, and ledger entries are not used.

*110. Rick checks the certificate for the site he is viewing and sees that it reads .example.com. What type of certificate is this, and why is it in use?  
A. It is a self-signed certificate, and it is used for testing purposes  
B. It is a wildcard certificate and is used for testing purposes  
C. It is a wildcard certificate and is used for multiple subdomains  
D. It is a self-signed certificate and is used for multiple subdomains****Answer: C. It is a wildcard certificate and is used for multiple subdomains*** *Explanation: A wildcard certificate (*.example.com) secures multiple subdomains, simplifying management. Self-signed certificates lack CA trust and aren’t used for subdomains.

**111. John wants to write a procedure that addresses what to do if an employee inadvertently discloses their password due to a phishing attempt. What type of control is John considering?**  
A. A directive control  
B. A proactive control  
C. A deterrent control  
D. A preventive control  
**Answer: A. A directive control**  
Explanation: Procedures guiding post-phishing actions are directive controls. Proactive controls are not a Security+ category, deterrents discourage attacks, and preventives stop incidents.

**112. Adam has been asked to implement an allow list for websites that his servers can visit. What concern should he raise about the implementation of allow lists?**  
A. Allow lists can be difficult to manage and cause failures if sites that are needed are not added  
B. Allow lists do not prevent sites from being visited if they are not on the allow list  
C. Allow lists cannot be configured to allow entire domains to be visited, creating significant overhead  
D. Allow lists are prone to error, allowing unwanted sites to be added  
**Answer: A. Allow lists can be difficult to manage and cause failures if sites that are needed are not added**  
Explanation: Allow lists require ongoing maintenance, risking failures if needed sites are omitted. They prevent unlisted sites, can allow domains, and errors don’t inherently allow unwanted sites.

**113. Jim wants to implement an authentication framework for his wireless network. Which of the following is most commonly used for wireless network authentication?**  
A. EAP  
B. MS-CHAP  
C. Kerberos  
D. LDAP  
**Answer: A. EAP**  
Explanation: Extensible Authentication Protocol (EAP) is standard for wireless authentication. MS-CHAP is for VPNs, Kerberos is for enterprise authentication, and LDAP is for directory services.

**114. Gary is preparing change management documentation for an application restart after patching. What step should immediately follow the application restart?**  
A. Validation testing  
B. Documenting the change occurred  
C. Updating version control  
D. Vulnerability scanning  
**Answer: A. Validation testing**  
Explanation: Validation testing ensures the application functions post-restart. Documentation, version control updates, and scanning follow or occur separately.

**115. Anna has been told that her organization has deployed microwave sensors in the organization’s warehouses. What are microwave sensors most frequently used to detect?**  
A. Motion  
B. Glass break  
C. Heat signatures  
D. Pressure  
**Answer: A. Motion**  
Explanation: Microwave sensors detect motion, penetrating walls for broad coverage. They don’t detect glass break, heat, or pressure.

**116. When is data on a drive that uses full-disk encryption at the greatest risk?**  
A. During the system boot process  
B. When the system is off  
C. When the system is logged in and in use  
D. When the system is being shut down  
**Answer: C. When the system is logged in and in use**  
Explanation: Full-disk encryption protects data when the system is off or locked. When logged in and in use, decrypted data is accessible, posing the greatest risk.

**117. Alex has configured full-disk encryption for laptops that his organization issues to employees. What cybersecurity objective does this primarily support?**  
A. Confidentiality  
B. Availability  
C. Authenticity  
D. Integrity  
**Answer: A. Confidentiality**  
Explanation: Full-disk encryption prevents unauthorized access, ensuring confidentiality. It doesn’t primarily address availability, authenticity, or integrity.

**118. What process reviews control objectives for an organization, system, or service to determine if controls do not meet the control objectives?**  
A. A penetration test  
B. A gap analysis  
C. A Boolean analysis  
D. A risk analysis  
**Answer: B. A gap analysis**  
Explanation: Gap analysis identifies discrepancies between control objectives and implemented controls. Penetration tests simulate attacks, Boolean analysis is not a security term, and risk analysis assesses threats.

**119. Frank configures an access control list to ensure that only specific IP addresses are able to connect to a service. What type of control has he deployed?**  
A. Managerial  
B. Physical  
C. Technical  
D. Operational  
**Answer: C. Technical**  
Explanation: ACLs are technical controls, restricting access via technology. Managerial controls are procedural, physical controls are tangible, and operational controls manage technology processes.

**120. Annie has recently implemented a video surveillance system for her organization. What is the largest driver for new ongoing costs for an unmonitored video surveillance system?**  
A. Camera maintenance  
B. The ongoing cost of storage  
C. Security guards  
D. Licensing  
**Answer: B. The ongoing cost of storage**  
Explanation: Video storage drives ongoing costs due to retention policies and resolution. Unmonitored systems don’t involve guards, maintenance is minimal, and licensing is less significant.

**121. Henry’s organization has recently experienced a ransomware attack and is restoring backups from a secure backup system. What type of security control is Henry using?**  
A. A preventive control  
B. A directive control  
C. A compensating control  
D. A corrective control  
**Answer: D. A corrective control**  
Explanation: Restoring backups corrects the ransomware issue, making it a corrective control. Preventive controls stop attacks, directive controls guide actions, and compensating controls address policy exceptions.

**122. What data obfuscation technique relies on a lookup table that allows you to match the data you want to secure to a randomly generated value to ensure that the actual value is not easily accessible?**  
A. Hashing  
B. Tokenization  
C. Randomization  
D. Masking  
**Answer: B. Tokenization**  
Explanation: Tokenization uses a lookup table to replace sensitive data with random tokens. Hashing is one-way, randomization is not a technique, and masking obscures partial data.

**123. What challenge drives the need for key exchange mechanisms?**  
A. The number of keys required for symmetric encryption  
B. The need to determine if a key is public  
C. The need to exchange keys in a way that prevents others from obtaining a copy  
D. The need to securely return keys to their owner after they are traded  
**Answer: C. The need to exchange keys in a way that prevents others from obtaining a copy**  
Explanation: Key exchange mechanisms (e.g., Diffie-Hellman) ensure secure key sharing without interception. Symmetric key counts, public key status, and key return are not primary concerns.

**124. Jackie is performing an impact analysis prior to a large-scale change her team is preparing to implement. Which of the following groups is not typically part of the impact analysis?**  
A. Stakeholders  
B. System administrators  
C. Service owners  
D. Legal counsel  
**Answer: D. Legal counsel**  
Explanation: Stakeholders, admins, and service owners assess change impacts. Legal counsel is involved in compliance, not routine impact analysis.

**125. Ilya wants to create a certificate signing request. Which of the following is not a typical part of a CSR?**  
A. The common name of the server  
B. The organization’s legal name  
C. A contact email address  
D. The organization’s phone number  
**Answer: D. The organization’s phone number**  
Explanation: CSRs include the common name, organization name, and email but not phone numbers, which are not required for certificate issuance.

**126. Before Tony stores a password hash, he appends a string of characters that is unique to each password generated using an algorithm he created. What technique is Tony using to help protect his password hashes?**  
A. Tokenization  
B. Steganography  
C. Salting  
D. Key stretching  
**Answer: C. Salting**  
Explanation: Salting adds unique random data to passwords before hashing, enhancing security. Tokenization replaces data, steganography hides data, and key stretching increases computation.

**127. Which of the following is not a step taken when a transaction is entered in a blockchain?**  
A. The value of the block is determined  
B. The transaction is sent to a peer-to-peer network of computers  
C. The transaction is validated using equations  
D. A transaction history is maintained as part of the blockchain  
**Answer: A. The value of the block is determined**  
Explanation: Blockchain transactions are sent to a P2P network, validated, and recorded in the ledger’s history. Block value is not a standard step in transaction processing.

**128. Kent wants to encrypt network traffic in transit. What cryptographic protocol is most frequently used to add encryption to existing protocols?**  
A. S/MIME  
B. TLS  
C. MPLS  
D. SSH  
**Answer: B. TLS**  
Explanation: TLS (Transport Layer Security) encrypts data in transit for various protocols (e.g., HTTPS). S/MIME is for email, MPLS is for routing, and SSH is for secure command-line access.

**129. Which of the following is not a common concern in change management processes related to legacy applications?**  
A. Lack of vendor support  
B. Lack of patches and updates  
C. Ongoing licensing costs  
D. Availability of third-party or consultant expertise  
**Answer: C. Ongoing licensing costs**  
Explanation: Legacy applications often lack vendor support, patches, and expertise but typically don’t incur ongoing licensing costs, as licenses are often perpetual or unavailable.

**130. Elaine wants to document the technical concerns that dependencies create as part of her change management process. Which of the following concerns is the most common when dependencies are encountered as part of change management?**  
A. Documenting the dependencies to ensure they are addressed  
B. Removing the dependencies as part of the change  
C. Patching the dependencies in addition to the main application  
D. Updating diagrams related to the dependencies  
**Answer: A. Documenting the dependencies to ensure they are addressed**  
Explanation: Documenting dependencies ensures they are accounted for during changes, preventing failures. Removing dependencies is rare, patching may not apply, and diagram updates are secondary.

**131. Gary has implemented record-level encryption for his database. How many keys will he use in a typical implementation of record-level encryption?**  
A. One key per record  
B. One key per column  
C. One key per table  
D. One key per database  
**Answer: A. One key per record**  
Explanation: Record-level encryption uses a unique key per record for granular security. Column, table, or database-level encryption uses fewer keys, reducing flexibility.

**132. Justin’s laptop is part of his organization’s zero-trust architecture. What term is used to refer to a device like a laptop, desktop, or mobile device in a zero-trust design?**  
A. A subject  
B. A policy engine  
C. A service provider  
D. A policy application point  
**Answer: A. A subject**  
Explanation: In zero-trust, devices like laptops are subjects, requiring continuous verification. Policy engines evaluate access, service providers are for federation, and policy application points are not standard terms.

**133. Susan’s organization has deployed a zero-trust architecture. Which of the following zero-trust control plane components uses rules to determine who can access a service based on the security status of their system, threat data, and similar information?**  
A. Adaptive authorization  
B. Threat scope reduction  
C. Policy-driven access control  
D. Secured zones  
**Answer: C. Policy-driven access control**  
Explanation: Policy-driven access control uses rules and data (e.g., system status, threat feeds) to grant access. Adaptive authorization adjusts dynamically, threat scope reduction limits attack surfaces, and secured zones are not control plane components.

**134. Scott wants to implement OCSP as part of an application he is creating. What will he implement?**  
A. A corrective control security process  
B. Certificate status checking  
C. Transport encryption  
D. Full-disk encryption  
**Answer: B. Certificate status checking**  
Explanation: OCSP (Online Certificate Status Protocol) checks certificate revocation status. It’s not a control, encryption, or disk-related process.

**135. Which of the following is not a common reason to implement key escrow?**  
A. Regulatory compliance  
B. Providing access to encrypted data for administrative reasons  
C. Providing access to encrypted data in emergencies  
D. Preventing the need for key rotation after a user leaves  
**Answer: D. Preventing the need for key rotation after a user leaves**  
Explanation: Key escrow supports compliance, administrative access, and emergencies but doesn’t prevent key rotation, which is still required post-departure.

**136. Yariv discovers that he has exposed his private key to other users in his organization by sending it via email instead of his public key. What should he do?**  
A. Ask the other users to delete any copies of his private key that they may have  
B. Immediately add his key to a CRL and reissue the key  
C. Create a new keypair and notify others that he has replaced his keypair  
D. Continue to operate as normal as long as the private key was not used maliciously  
**Answer: C. Create a new keypair and notify others that he has replaced his keypair**  
Explanation: A compromised private key requires a new keypair and notification to ensure secure communication. Deleting copies is unreliable, CRLs are for certificates, and continuing is insecure.

**137. What happens if a mistake is made and an incorrect transaction is entered into the open public ledger in a blockchain?**  
A. The transaction is reversed once it is discovered, and the original transaction is removed from the record  
B. A new transaction must be processed, and both transactions remain in the record  
C. The original transaction is updated and becomes the new record  
D. An error lock must be mined and labeled with the transaction number and error details  
**Answer: B. A new transaction must be processed, and both transactions remain in the record**  
Explanation: Blockchains are immutable; errors require a new transaction, and both remain in the ledger. Reversals, updates, or error locks are not standard blockchain processes.

**138. Which of the following activities will not typically result in a need to update policies and procedures?**  
A. Deploying a new application  
B. Installing patches for an existing application  
C. Conducting a lessons learned exercise after an incident  
D. Changes in regulations  
**Answer: B. Installing patches for an existing application**  
Explanation: Patching rarely changes policies/procedures. New applications, incident lessons, and regulatory changes often require updates.

**139. Hrant’s organization wants to ensure that staff members use both something they know and something they have as part of their physical access control scheme. Which of the following solutions meets that requirement?**  
A. Security guards and access badges  
B. Keys and access control vestibules  
C. Access badges and PINs  
D. Security guards and access control vestibules  
**Answer: C. Access badges and PINs**  
Explanation: Badges (something you have) and PINs (something you know) provide two-factor authentication. Guards and vestibules don’t inherently meet both criteria.

**140. Julia wants to detect if an intruder enters a space using a sensor system. Which of the following is not typically used to detect intruders?**  
A. Infrared sensors  
B. Ultrasonic sensors  
C. Microwave sensors  
D. Pressure sensors  
**Answer: D. Pressure sensors**  
Explanation: Infrared, ultrasonic, and microwave sensors detect intruders via motion or presence. Pressure sensors are used for specific applications like footsteps, not general intruder detection.

**141. Which of the following is not true for a secure cryptographic hash system?**  
A. Hashes are a one-way function  
B. Hashes generate a fixed length output  
C. Hashes may generate the same output for multiple inputs  
D. Hashes are commonly used to verify the integrity of files  
**Answer: C. Hashes may generate the same output for multiple inputs**  
Explanation: Secure hashes (e.g., SHA-256) are designed to avoid collisions (same output for different inputs). They are one-way, fixed-length, and used for integrity verification.

**142. Casey wants to prevent tailgating attacks on her datacenter. What type of physical security solution should she put in place?**  
A. Video surveillance  
B. Bollards  
C. An access control vestibule  
D. Access badges  
**Answer: C. An access control vestibule**  
Explanation: Access control vestibules prevent tailgating by requiring sequential door authentication. Surveillance detects, bollards stop vehicles, and badges don’t address tailgating.

**143. As Casey continues to work to secure her datacenter, she decides to deploy access badges. What technique will provide the greatest assurance that a stolen or cloned access badge will not allow an attacker access?**  
A. Use barcode-based badges  
B. Require a PIN along with the badge  
C. Use RFID-based badges  
D. Include a picture of the user on the badge  
**Answer: B. Require a PIN along with the badge**  
Explanation: A PIN (something you know) with a badge (something you have) adds two-factor authentication, preventing stolen badge misuse. Barcodes/RFID don’t add security, and pictures rely on human verification.

**144. What term describes the function of digital signatures related to proving that the signature was provided by the owner of a given private key?**  
A. Ledger-based validation  
B. Nonrepudiation  
C. Key stretching  
D. Authentication  
**Answer: B. Nonrepudiation**  
Explanation: Digital signatures provide nonrepudiation, proving the signer’s identity via their private key. Ledger-based validation, key stretching, and authentication are unrelated or incorrect.

**145. John wants to send his public key to another user. What steps are necessary to do so?**  
A. The key must be sent using Diffie-Hellman  
B. The key can simply be sent via email or other means  
C. The key must be sent using RSA  
D. The key must be signed, then sent via email or other means  
**Answer: B. The key can simply be sent via email or other means**  
Explanation: Public keys are safe to share openly (e.g., via email). Diffie-Hellman and RSA are for key exchange, and signing is unnecessary for public keys.

**146. Tracy wants to use the most secure salting solution she can. Which of the following options will provide the most secure salt?**  
A. Set a salt value and store it in the program code  
B. Generate a unique salt for each hashed entry  
C. Generate a unique salt value every time a value is used  
D. Use a fixed salt stored in a database  
**Answer: B. Generate a unique salt for each hashed entry**  
Explanation: Unique salts per hash maximize security by preventing rainbow table attacks. Fixed salts or repeated salts reduce effectiveness, and per-use salts are impractical.

**147. Bob conducts a periodic risk assessment of his organization. What category of security control is this?**  
A. Technical  
B. Managerial  
C. Operational  
D. Physical  
**Answer: B. Managerial**  
Explanation: Risk assessments are managerial controls, focusing on risk management processes. Technical controls are technology-based, operational controls manage tech securely, and physical controls are tangible.

**148. After a breach, Jackie removes malicious software from a server that she is responsible for. What control type should she classify this as?**  
A. Preventive  
B. Corrective  
C. Compensating  
D. Deterrent  
**Answer: B. Corrective**  
Explanation: Removing malware corrects a security issue, making it a corrective control. Preventive controls stop issues, compensating controls address exceptions, and deterrents discourage attacks.

**149. What can a root SSL (TLS) certificate do?**  
A. Remove a certificate from a CRL  
B. Generate a signing key and use it to sign a new certificate  
C. Authorize new CA users  
D. Allow key stretching  
**Answer: B. Generate a signing key and use it to sign a new certificate**  
Explanation: Root certificates sign subordinate certificates, establishing trust. They don’t manage CRLs, authorize users, or perform key stretching.

**150. Christina wants to authenticate individuals as part of her AAA implementation. What will she need to do to authenticate users?**  
A. Match users to roles and ensure that rights are assigned  
B. Conduct biometric enrollments for every user  
C. Use identity proofing for each user she creates  
D. Ensure that users provide an identity and one or more authentication factors  
**Answer: D. Ensure that users provide an identity and one or more authentication factors**  
Explanation: Authentication requires users to claim an identity and provide factors (e.g., password, biometrics). Role matching is authorization, biometric enrollment is optional, and identity proofing is for onboarding.