Certified Information Systems Security Professional

1. Physical assets defined in an organization's business impact analysis (BIA) could include which of the following?

A. Personal belongings of organizational staff members

B. Disaster recovery (DR) line-item revenues

C. Cloud-based applications

D. Supplies kept off-site a remote facility

Answer(s): D

---

2. When assessing the audit capability of an application, which of the following activities is MOST important?

A. Identify procedures to investigate suspicious activity.

B. Determine if audit records contain sufficient information.

C. Verify if sufficient storage is allocated for audit records.

D. Review security plan for actions to be taken in the event of audit failure.

Answer(s): B

---

3. An organization would like to implement an authorization mechanism that would simplify the assignment of various system access permissions for many users with similar job responsibilities. Which type of authorization mechanism would be the BEST choice for the organization to implement?

A. Role-based access control (RBAC)

B. Discretionary access control (DAC)

C. Content-dependent Access Control

D. Rule-based Access Control

Answer(s): A

---

4. What is the PRIMARY reason for criminal law being difficult to enforce when dealing with cybercrime?

A. Jurisdiction is hard to define.

B. Law enforcement agencies are understaffed.

C. Extradition treaties are rarely enforced.

D. Numerous language barriers exist.

Answer(s): A

---

5. Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

A. Extensible Authentication Protocol (EAP)

B. Internet Protocol Security (IPsec)

C. Secure Sockets Layer (SSL)

D. Secure Shell (SSH)

Answer(s): A

---

6. Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

A. Reference monitor

B. Trusted Computing Base (TCB)

C. Time separation

D. Security kernel

Answer(s): D

---

7. What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

A. Performance testing

B. Risk assessment

C. Security audit

D. Risk management

Answer(s): D

---

8. Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this IAM action?

A. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identity provider (IdP) and allows access to resources.

D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to resources.

Answer(s): B

---

9. Which of the following statements BEST describes least privilege principle in a cloud environment?

A. A single cloud administrator is configured to access core functions.

B. Internet traffic is inspected for all incoming and outgoing packets.

C. Routing configurations are regularly updated with the latest routes.

D. Network segments remain private if unneeded to access the internet.

Answer(s): D

---

10. An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Compression

B. Caching

C. Replication

D. Deduplication

Answer(s): D

---

11. Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

A. Synchronous Optical Networking (SONET)

B. Multiprotocol Label Switching (MPLS)

C. Fiber Channel Over Ethernet (FCoE)

D. Session Initiation Protocol (SIP)

Answer(s): B

---

12. Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

A. File Integrity Checker

B. Security information and event management (SIEM) system

C. Audit Logs

D. Intrusion detection system (IDS)

Answer(s): A

---

13. Which of the following is included in change management?

A. Technical review by business owner

B. User Acceptance Testing (UAT) before implementation

C. Cost-benefit analysis (CBA) after implementation

D. Business continuity testing

Answer(s): D

---

14. A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

A. Pinning

B. Single-pass wipe

C. Multi-pass wipes

D. Degaussing

Answer(s): C

---

15. When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

A. SOC 1 Type 1

B. SOC 2 Type 1

C. SOC 2 Type 2

D. SOC 3

Answer(s): C

---

16. Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

A. Instant messaging or chat applications

B. Peer-to-Peer (P2P) file sharing applications

C. E-mail applications

D. End-to-end applications

Answer(s): B

---

17. An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 0

B. 1

C. 2

D. 3

Answer(s): B

---

18. Which of the following is the BEST way to protect an organization's data assets?

A. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.

B. Monitor and enforce adherence to security policies.

C. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

D. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.

Answer(s): A

---

19. Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

A. Training department

B. Internal audit

C. Human resources

D. Information technology (IT)

Answer(s): C

---

20. Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

A. Control traffic

B. Control air flow

C. Prevent piggybacking

D. Prevent rapid movement

Answer(s): C
