Isaca Cybersecurity-Audit-Certificate Practice Questions

Shared by Arnold on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following BIST enables continuous identification and mitigation of security threats to an organization?

Options:

A- demit/ and access management (1AM)
B- Security operations center (SOC)
C- Security training and awareness
D- Security information and event management (SEM)

Answer:

B

Explanation:

Asecurity operations center (SOC)is a centralized unit that monitors, detects, analyzes, and responds to cyber threats and incidents in real time. A SOC enables continuous identification and mitigation of security threats to an organization by using various tools, processes, and expertise.

Question 2

Question Type: MultipleChoice

Which option best describes specific, mandatory controls or rules to support and comply with a policy?

Options:

A- Frameworks
B- Guidelines
C- Basedine
D- Standards

Answer:

D

Explanation:

Specific, mandatory controls or rules to support and comply with a policy are known as standards. This is because standards define the minimum level of performance or behavior that is expected from an organization or its employees in order to achieve a policy objective or requirement. Standards also provide clear and measurable criteria for auditing and monitoring compliance with policies. The other options are not specific, mandatory controls or rules to support and comply with a policy, but rather different types of documents or tools that provide guidance or recommendations for implementing policies or controls, such as frameworks (A), guidelines (B), or baselines C.

Question 3

Question Type: MultipleChoice

At which layer in the open systems interconnection (OSI) model does SSH operate?

Options:

A- Presentation
B- Session
C- Application
D- Network

Answer:

C

Explanation:

SSH, or Secure Shell, is a network protocol that operates at the Application layer of the OSI model. This is the topmost layer, which allows users to interact with the network through applications. SSH provides a secure channel over an unsecured network in a client-server architecture, enabling users to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Question 4

Question Type: MultipleChoice

Which of the following is the PRIMARY goal of implementing a change management process?

Options:

A- To ensure changes are communicated to the process owners prior to going live
B- To minimize disruptions to the business from system changes
C- To ensure that changes made to a system are performed on schedule
D- To validate that changes to the system provide the expected return on investment

Answer:

B

Explanation:

Change management processes are designed to ensure that changes are introduced in a controlled and coordinated manner. The main objective is to minimize the impact of changes on the business and its operations. This involves careful planning, testing, communication, and implementation to ensure that business processes continue to operate smoothly during and after the transition.

Question 5

Question Type: MultipleChoice

Which option best provides additional protection other than encryption to messages transmitted using portable wireless devices?

Options:

A- Endpoint protection
B- Intrusion detection system (IDS)
C- Virtual private network (VPN)
D- Intrusion prevention system (IPS)

Answer:

C

Explanation:

A Virtual Private Network (VPN) provides additional protection to messages transmitted using portable wireless devices by creating a secure and encrypted tunnel for data transmission. This helps protect the data from being intercepted or accessed by unauthorized entities. While encryption secures the content of the messages, a VPN secures the transmission path, adding an extra layer of security.

Question 6

Question Type: MultipleChoice

The GREATEST advantage of using a common vulnerability scoring system is that it helps with:

Options:

A- risk aggregation.
B- risk prioritization.
C- risk elimination.
D- risk quantification

Answer:

B

Explanation:

The GREATEST advantage of using a common vulnerability scoring system is that it helps with risk prioritization. This is because a common vulnerability scoring system provides a standardized and consistent way of measuring and comparing the severity of vulnerabilities, based on their impact and exploitability. This allows organizations to prioritize the remediation of the most critical vulnerabilities and allocate resources accordingly. The other options are not as advantageous as using a common vulnerability scoring system, because they either involve aggregating (A), eliminating C, or quantifying (D) risk, which are not directly related to the scoring system.

Question 7

Question Type: MultipleChoice

Which option best contains the essential elements of effective processes and describes an improvement path considering quality and effectiveness?

Options:

A- Capability maturity model integration
B- Balanced scorecard
C- 60 270042009
D- COBIT 5

Answer:

A

Explanation:

The document that contains the essential elements of effective processes and describes an improvement path considering quality and effectiveness is Capability Maturity Model Integration (CMMI). This is because CMMI is a framework that defines five levels of process maturity, from initial to optimized, and provides best practices and guidelines for improving the quality and effectiveness of processes across different domains, such as software development, service delivery, or cybersecurity. The other options are not documents that contain the essential elements of effective processes and describe an improvement path considering quality and effectiveness, but rather different types of documents or tools that provide guidance or recommendations for implementing policies or controls, such as Balanced Scorecard (B), ISO 27004:2009 C, or COBIT 5 (D).

Question 8

Question Type: MultipleChoice

When reviewing user management roles, Which option best groups presents the GREATEST risk based on their permissions?

Options:

A- Privileged users
B- Database administrators
C- Terminated employees
D- Contractors

Answer:

A

Explanation:

When reviewing user management roles, the group that presents the GREATEST risk based on their permissions is privileged users. This is because privileged users are users who have elevated or special access rights or permissions to systems or resources, such as administrators, superusers, root users, etc. Privileged users present the greatest risk based on their permissions, because they can perform actions or operations that can affect the security, availability, or functionality of systems or resources, such as installing or uninstalling software, modifying or deleting files, granting or revoking access rights, etc. Privileged users can also abuse or misuse their permissions for malicious or unauthorized purposes, such as stealing or leaking sensitive data, sabotaging systems or services, bypassing security controls, etc. The other options are not groups that present the greatest risk based on their permissions, but rather different types of users that may have different levels of access rights or permissions to systems or resources, such as database administrators (B), terminated employees C, or contractors (D).

Question 9

Question Type: MultipleChoice

Which of the following is a MAIN benefit of using Security as a Service (SECaaS) providers?

Options:

A- Significant investments and specialized security skills are not required.
B- Enterprises can use the latest technologies to counter threats that are constantly evolving.
C- SECaaS providers are compliant with specific security requirements and new regulations.
D- Available security services from providers are affordable to enterprises of all sizes.

Answer:

A

Explanation:

A MAIN benefit of using Security as a Service (SECaaS) providers is thatsignificant investments and specialized security skills are not required. SECaaS is a type of cloud service model that provides security solutions and services to customers over the internet. SECaaS providers can offer various security functions such as antivirus, firewall, encryption, identity management, vulnerability scanning, and incident response. By using SECaaS providers, customers can save costs and resources on acquiring, maintaining, and updating security hardware and software. Customers can also leverage the expertise and experience of the SECaaS providers to address their security needs and challenges.

Question 10

Question Type: MultipleChoice

In cloud computing, which type of hosting is MOST appropriate for a large organization that wants greater control over the environment?

Options:

A- Private hosting
B- Public hosting
C- Shared hosting
D- Hybrid hosting

Answer:

A

Explanation:

In cloud computing, the type of hosting that is MOST appropriate for a large organization that wants greater control over the environment isprivate hosting. Private hosting is a type of cloud service model where the cloud infrastructure is dedicated to a single organization and hosted either on-premise or off-premise by a third-party provider. Private hosting offers more control over the security, performance, customization, and compliance of the cloud environment than other types of hosting.

Question 11

Question Type: MultipleChoice

Which option best BEST characterizes security mechanisms for mobile devices?

Options:

A- Easy to control through mobile device management
B- Comparatively weak relative to workstations
C- Inadequate for organizational use
D- Configurable and reliable across device types

Answer:

A

Explanation:

The BEST characteristic that describes security mechanisms for mobile devices is easy to control through mobile device management. This is because mobile device management is a technique that allows organizations to centrally manage and secure mobile devices, such as smartphones, tablets, laptops, etc., that are used by their employees or customers. Mobile device management helps to enforce security policies, configure settings, install applications, monitor usage, wipe data, etc., on mobile devices remotely and efficiently. The other options are not characteristics that describe security mechanisms for mobile devices, but rather different aspects or factors that affect security mechanisms for mobile devices, such as weakness (B), inadequacy C, or reliability (D).

Question 12

Question Type: MultipleChoice

Which of the following costs are typically covered by cybersecurity insurance?

Options:

A- Forensic investigation
B- Threat intelligence feed
C- SIEM implementation

D- Reputational loss

Answer:

A

Explanation:

Cybersecurity insurance typically covers direct and immediate losses due to data breaches and information security breaches. This often includes legal costs, credit monitoring costs, litigation costs (such as breach of privacy), and costs of regulatory investigations. Forensic investigation is a critical component of the response to a cyber incident, and the costs associated with it are generally covered under a cybersecurity insurance policy.

Question 13

Question Type: MultipleChoice

An organization's responsibility to protect its assets and operations, including IT infrastructure and information, is referred to as:

Options:

A- corporate risk management and assurance strategy.
B- cybersecurity goals, objectives, and mission.
C- organizational cybersecurity policies and procedures.
D- governance, risk management, and compliance.

Answer:

D

Explanation:

The responsibility of an organization to protect its assets, including IT infrastructure and information, falls under the broader umbrella of governance, risk management, and compliance (GRC). Governance ensures that organizational activities, like managing IT operations, are aligned with the business's goals, risk management involves identifying, assessing, and mitigating risks, and compliance ensures that the organization adheres to laws, regulations, and policies.

Reference= While I can't provide direct references from the Cybersecurity Audit Manual, the concept of GRC is widely recognized in cybersecurity frameworks and best practices, such as those outlined by ISACA and other industry standards.