IIBA-CCA Practice Test

Shared by Cleveland on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SSL/TLS encryption capability is provided by:

Options:

A- certificates.
B- protocols.
C- passwords.
D- controls.

Answer:

B

Explanation:

SSL and its successor TLS are cryptographic protocols designed to provide secure communications over untrusted networks. The encryption capability comes from the TLS protocol suite, which defines how two endpoints negotiate security settings, authenticate, exchange keys, and protect data as it travels between them. During the TLS handshake, the endpoints agree on a cipher suite, establish shared session keys using secure key exchange methods, and then use symmetric encryption and integrity checks to protect application data against eavesdropping and tampering. Because TLS specifies these mechanisms and the sequence of steps, it is accurate to say that encryption capability is provided by protocols.

Certificates are important but they are not the encryption mechanism itself. Digital certificates primarily support authentication and trust by binding a public key to an identity and enabling verification through a trusted certificate authority chain. Certificates help prevent impersonation and man-in-the-middle attacks by allowing clients to validate the server's identity, and in mutual TLS they can validate both parties. However, certificates alone do not define how encryption is negotiated or applied; TLS does.

Passwords are unrelated to transport encryption; they are an authentication secret and do not provide session encryption for network traffic. ''Controls'' is too general: SSL/TLS is indeed a security control, but the question asks specifically what provides the encryption capability. That capability is implemented and standardized by the SSL/TLS protocols, which orchestrate key establishment and encrypted communication.

Question 2

Question Type: MultipleChoice

What risk to information integrity is a Business Analyst aiming to minimize, by defining processes and procedures that describe interrelations between data sets in a data warehouse implementation?

Options:

A- Unauthorized Access
B- Confidentiality
C- Data Aggregation
D- Cross-Site Scripting

Answer:

C

Explanation:

In a data warehouse, information from multiple operational sources is consolidated, transformed, and related through keys, joins, and business rules. When a Business Analyst defines processes and procedures that describe how data sets interrelate, they are primarily controlling the risk created by data aggregation. Aggregation risk arises when combining multiple datasets produces a new, richer dataset that can change the meaning, sensitivity, or trustworthiness of the information. If relationships and transformation rules are poorly defined or inconsistently applied, the warehouse can generate misleading analytics, incorrect roll-ups, duplicated records, or invalid correlations---directly harming information integrity because decisions are made on inaccurate or improperly combined data.

Well-defined interrelation procedures specify authoritative sources, master data rules, key management, referential integrity expectations, transformation and reconciliation steps, and data lineage. These controls help ensure the warehouse preserves correctness when data is integrated across systems with different formats, definitions, and update cycles. They also support governance by enabling validation checks (for example, balancing totals to source systems, exception handling, and data-quality thresholds) and by making it clear which dataset should be trusted for specific attributes.

Unauthorized access and confidentiality are important warehouse risks, but they are addressed mainly through access controls and encryption. Cross-site scripting is a web application vulnerability and is not the core issue in describing dataset relationships. Therefore, the correct answer is Data Aggregation.

Question 3

Question Type: MultipleChoice

A software product that supports threat detection, and compliance and security incident management, through the collection and analysis of security events and other data sources, is known as a:

Options:

A- software as a service (SaaS).
B- threat risk assessment (TRA).
C- security information and event management system (SIEM).
D- cloud access security broker (CASB).

Answer:

C

Explanation:

A security information and event management system (SIEM) is designed to centralize and analyze security-relevant data to support threat detection, compliance reporting, and incident management. SIEM platforms ingest logs and telemetry from many sources such as servers, endpoints, network devices, firewalls, intrusion detection systems, identity providers, cloud services, and business applications. They normalize and correlate these events so analysts can identify suspicious patterns that would be difficult to see in isolated logs, such as repeated failed logins followed by a successful login from an unusual location, privilege escalation, lateral movement indicators, or abnormal data access.

Cybersecurity operational guidance emphasizes SIEM value in three main areas. First, detection and alerting: correlation rules, behavioral analytics, and threat intelligence enrichment help surface high-risk activity. Second, incident response support: SIEM provides timelines, evidence preservation, triage context, and query capabilities that help responders scope and contain incidents. Third, compliance and audit readiness: centralized log retention, integrity controls, and reporting demonstrate that monitoring and control requirements are operating.

The other options do not match the definition. SaaS is a delivery model, not a specific security monitoring capability. A threat risk assessment is a process, not a software product for event collection and correlation. A CASB focuses on governing and protecting cloud application usage, whereas SIEM focuses on cross-environment event aggregation, correlation, and security operations monitoring.

Question 4

Question Type: MultipleChoice

What is risk mitigation?

Options:

A- Reducing the risk by implementing one or more countermeasures
B- Purchasing insurance against a cybersecurity breach
C- Eliminating the risk by stopping the activity which causes risk
D- Documenting the risk in full and preparing a recovery plan

Answer:

A

Explanation:

Risk mitigation is the risk treatment approach focused on reducing risk to an acceptable level by lowering either the likelihood of a risk event, the impact of that event, or both. In cybersecurity risk management, mitigation is accomplished by implementing controls and countermeasures such as technical safeguards, process changes, and administrative measures. Examples include patching vulnerable systems, hardening configurations, enabling multi-factor authentication, applying least privilege, network segmentation, encryption, improved logging and monitoring, secure development practices, and user awareness training. Each of these actions reduces exposure or limits damage if an incident occurs.

The other options describe different risk treatment strategies, not mitigation. Purchasing insurance is generally considered risk transfer, where financial impact is shifted to a third party, but the underlying threat and vulnerability may still exist. Eliminating risk by stopping the risky activity is risk avoidance; it removes the exposure by discontinuing the process, system, or behavior causing the risk. Documenting the risk and preparing a recovery plan aligns more closely with risk acceptance combined with contingency planning or resilience planning; it acknowledges the risk and focuses on recovery rather than reducing the probability of occurrence.

Therefore, the correct definition of risk mitigation is reducing the risk through implementing one or more countermeasures.

Question 5

Question Type: MultipleChoice

What is defined as an internal computerized table of access rules regarding the levels of computer access permitted to login IDs and computer terminals?

Options:

A- Access Control List
B- Access Control Entry
C- Relational Access Database
D- Directory Management System

Answer:

A

Explanation:

An Access Control List (ACL) is a structured, system-maintained list of authorization rules that specifies who or what is allowed to access a resource and what actions are permitted. In many operating systems, network devices, and applications, an ACL functions as an internal table that maps identities such as user IDs, group IDs, service accounts, or even device/terminal identifiers to permissions like read, write, execute, modify, delete, or administer. When a subject attempts to access an object, the system consults the ACL to determine whether the requested operation should be allowed or denied, enforcing the organization's security policy at runtime.

The description in the question matches the classic definition of an ACL as a computerized table of access rules tied to login IDs and sometimes the originating endpoint or terminal context. ACLs are central to implementing discretionary access control and are also widely used in networking (for example, permitting or denying traffic flows based on source/destination and ports) and file systems (controlling access to folders and files).

An Access Control Entry (ACE) is only a single line item within an ACL (one rule for one subject). A ''Relational Access Database'' is not a standard security control term for authorization tables. A ''Directory Management System'' manages identities and groups, but it is not the same as the enforcement list attached to a specific resource. Therefore, the correct answer is Access Control List.

Question 6

Question Type: MultipleChoice

Analyst B has discovered multiple sources which can harm the organization's systems. What has she discovered?

Options:

A- Breach
B- Hacker
C- Threat
D- Ransomware

Answer:

C

Explanation:

Multiple sources that can harm an organization's systems are classified as threats. In cybersecurity risk terminology, a threat is any circumstance, event, actor, or condition with the potential to adversely impact confidentiality, integrity, or availability. Threats can be human (external attackers, insiders, third-party compromises), technical (malware, ransomware campaigns, exploit kits), operational (misconfigurations, weak processes, inadequate monitoring), or environmental (power disruption, natural disasters). This differs from a breach, which is the realized outcome where unauthorized access or disclosure has already occurred. It also differs from hacker, which refers to one type of threat actor rather than the broader category of potential harm. Ransomware is a specific threat type (malware that encrypts data and demands payment), not a general term for multiple sources of harm. Cybersecurity documents commonly pair ''threats'' with ''vulnerabilities'' and ''controls'': threats exploit vulnerabilities to create risk; controls reduce either the likelihood of exploitation or the impact if exploitation occurs. Identifying ''multiple sources which can harm systems'' is essentially threat identification--an early and ongoing step in risk management used to inform security architecture, monitoring, and incident preparedness. Therefore, the correct concept is threat.

Question 7

Question Type: MultipleChoice

The opportunity cost of increased cybersecurity is that:

Options:

A- cybersecurity adds considerably to the cost of developing new business systems.
B- costs of meeting regulations are constantly increasing.
C- the potential cost of implementing security will always be less than the potential risk from a breach of customer data.
D- identifying and securing assets and systems requires resources that are therefore not available to other initiatives.

Answer:

D

Explanation:

Opportunity cost is a core enterprise-risk and economics concept: when an organization allocates limited resources to one activity, it reduces what is available for other priorities. Increasing cybersecurity typically requires money, skilled personnel time, executive attention, tooling, and operational capacity. Those resources could otherwise be used for revenue-generating work such as new product features, customer experience improvements, system modernization, market expansion, or process automation. That tradeoff is exactly what option D describes, making it the correct answer.

Cybersecurity documents stress that risk treatment decisions must balance risk reduction against cost, feasibility, and business impact. While stronger security can reduce the likelihood and impact of incidents, it can also introduce friction (extra approval steps, stronger authentication, segmentation), slow delivery when changes require additional reviews, and demand ongoing operational effort (monitoring, patching, vulnerability remediation, access recertification, incident response testing). These impacts are not arguments against security; they are the reason governance processes prioritize controls based on the most critical assets, highest-risk threats, and compliance requirements.

Option A may be true in some cases, but it describes a direct cost, not the broader economic concept of opportunity cost. Option B is a trend statement and not the definition. Option C is incorrect because security spend is not always less than breach risk; organizations must evaluate cost-benefit and acceptable residual risk rather than assume a universal rule.

Question 8

Question Type: MultipleChoice

Which organizational area would drive a cybersecurity infrastructure Business Case?

Options:

A- Risk
B- IT
C- Legal
D- Finance

Answer:

A

Explanation:

A cybersecurity infrastructure business case is typically driven by the Risk function because the justification for security investments is grounded in reducing enterprise risk to an acceptable level and aligning with the organization's risk appetite and regulatory obligations. Risk-focused teams (often working with the CISO and security governance) translate threats, vulnerabilities, and control gaps into business impact terms such as likelihood of adverse events, potential operational disruption, financial exposure, regulatory penalties, and reputational harm. This framing is what a formal business case requires: a clear problem statement, quantified or prioritized risk scenarios, expected risk reduction from proposed controls, and how residual risk compares to tolerance thresholds.

While IT usually leads implementation and provides architecture, sizing, and operational cost estimates, IT alone does not typically ''drive'' the business case without the risk rationale that explains why the investment is necessary and what enterprise outcomes it protects. Legal contributes requirements related to compliance, contracts, and breach handling, but it generally supports rather than owns investment prioritization. Finance evaluates budgeting, funding options, and return-on-investment assumptions, yet it relies on risk inputs to understand why the spend is warranted and what loss exposure is being reduced.

Therefore, the organizational area most responsible for driving a cybersecurity infrastructure business case---by defining the risk problem, articulating risk-based benefits, and enabling executive decision-making---is Risk.

Bottom of Form

Question 9

Question Type: MultipleChoice

What does non-repudiation mean in the context of web security?

Options:

A- Ensuring that all traffic between web servers must be securely encrypted
B- Providing permission to use web server resources according to security policies and specified procedures, so that the activity can be audited
C- Ensuring that all data has not been altered in an unauthorized manner while being transmitted between web servers
D- Providing the sender of a message with proof of delivery, and the receiver with proof of the sender's identity

Answer:

D

Explanation:

Non-repudiation is a security property that provides verifiable evidence of an action or communication so that the parties involved cannot credibly deny their participation later. In web security, it most commonly means being able to prove who sent a message or performed a transaction and, in many cases, that the message was received and recorded. This is why option D is correct: it captures the idea of giving the receiver proof of the sender's identity and giving the sender evidence that the message or transaction was delivered or accepted.

Cybersecurity guidance typically associates non-repudiation with digital signatures, strong identity binding, and protected audit evidence. A digital signature uses asymmetric cryptography so that only the holder of a private key can sign, while anyone with the public key can verify the signature. When combined with trusted certificates, accurate time sources, and protected logs, this creates strong accountability. Non-repudiation also depends on maintaining the integrity of supporting evidence, such as tamper-resistant audit logs, secure log retention, and controlled access to signing keys.

It is different from confidentiality (encryption of traffic), and different from integrity alone (preventing unauthorized modification). It is also different from authorization and auditing, which support accountability but do not, by themselves, provide cryptographic-grade proof that a specific entity performed a specific action. Non-repudiation is especially important for high-trust transactions such as approvals, payments, and legally binding communications.

Question 10

Question Type: MultipleChoice

Where business process diagrams can be used to identify vulnerabilities within solution processes, what tool can be used to identify vulnerabilities within solution technology?

Options:

A- Vulnerability-as-a-Service
B- Penetration Test
C- Security Patch
D- Smoke Test

Answer:

B

Explanation:

Business process diagrams help analysts spot weaknesses in workflows, approvals, handoffs, and segregation of duties, but they do not directly test the technical security of the underlying applications, infrastructure, or configurations. To identify vulnerabilities within solution technology, cybersecurity practice uses penetration testing, which is a controlled, authorized simulation of real-world attacks against systems. A penetration test examines how a solution behaves under adversarial conditions and validates whether security controls actually prevent exploitation, not just whether they are designed on paper.

Penetration testing typically includes reconnaissance, enumeration, and attempts to exploit weaknesses in areas such as authentication, session management, access control, input handling, APIs, encryption usage, misconfigurations, and exposed services. Results provide evidence-based findings, including exploit paths, impact, affected components, and recommended remediations. This makes penetration testing especially valuable before go-live, after major changes, and periodically for high-risk systems to confirm the security posture remains acceptable.

The other options do not fit the objective. A security patch is a remediation action taken after vulnerabilities are known, not a method for discovering them. A smoke test is a basic functional check to confirm the system builds and runs; it is not a security assessment. Vulnerability-as-a-Service is a delivery model that may include scanning or testing, but the recognized tool or technique for identifying vulnerabilities in the technology itself in this context is a penetration test, which directly evaluates exploitability and real security impact.