



IIBA-CCA Practice Questions

Shared by Boyle on 09-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Which organizational resource category is known as "the first and last line of defense" from an attack?

Options:

- A- Firewalls
- B- Employees
- C- Endpoint Devices
- D- Classified Data



Answer:

B

Explanation:

In cybersecurity guidance, employees are often described as the first and last line of defense because human actions influence nearly every stage of an attack. They are the first line since many threats begin with user interaction: phishing emails, malicious links, social engineering calls, unsafe file handling, weak passwords, and accidental disclosure of sensitive information. A well-trained user who recognizes suspicious requests, verifies identities, and reports anomalies can stop an incident before any technical control is even engaged.

Employees are also the last line because technical protections such as firewalls, filters, and endpoint tools are not perfect. Attackers routinely bypass or evade automated defenses using stolen credentials, living-off-the-land techniques, misconfigurations, or novel malware. When those controls fail, the organization still depends on people to apply secure behaviors: following least privilege, protecting credentials, using multifactor authentication correctly, confirming out-of-band requests for payments or data, and escalating unusual activity quickly. Incident response, containment, and recovery also depend on humans making correct decisions under pressure, following documented procedures, and communicating accurately.

Cybersecurity documents emphasize that a strong security culture, regular awareness training, role-based education, clear reporting channels, and consistent policy enforcement reduce human-enabled risk and turn employees into an effective security control rather than a vulnerability.

Question 2

Question Type: MultipleChoice

ITIL Information Technology Infrastructure Library defines:

Options:

- A- a standard of best practices for IT Service Management.
- B- how technology and hardware systems interface securely with one another.
- C- the standard set of components used in every business technology system.
- D- a set of security requirements that every business technology system must meet.

Answer:

A

Explanation:

ITIL is a widely adopted framework that defines best-practice guidance for IT Service Management. Its focus is on how organizations design, deliver, operate, and continually improve IT services so they reliably support business outcomes. In cybersecurity and service delivery documentation, ITIL is often referenced because strong service management processes are foundational to secure operations. For example, ITIL practices such as incident management, problem management, change enablement, configuration management, and service continuity help ensure security controls are implemented consistently and that deviations are identified, tracked, and corrected.

ITIL does not define how hardware systems interface securely with one another; that is more aligned with architecture standards, security engineering, and network or platform design frameworks. It also does not prescribe a universal set of components for every technology system; that belongs to reference architectures and enterprise architecture standards. Likewise, ITIL is not primarily a security requirements standard. While ITIL supports security governance through practices like risk management, access management, and information security management integration, it does not itself serve as a mandatory security control catalog.

From a cybersecurity perspective, ITIL contributes by promoting repeatable processes, clear roles and responsibilities, measurable service levels, and continual improvement. These elements reduce operational risk, improve response effectiveness, and strengthen accountability---key requirements for maintaining confidentiality, integrity, and availability in production environments.

Question 3

Question Type: MultipleChoice

Cybersecurity regulations typically require that enterprises demonstrate that they can protect:

Options:

- A- applications and technology systems.
- B- trade secrets and other intellectual property.
- C- personal data of customers and employees.
- D- business continuity and disaster recovery.

Answer:

C

Explanation:

Cybersecurity regulations most commonly focus on the protection of personal data, because misuse or exposure can directly harm individuals through identity theft, fraud, discrimination, or loss of privacy. Privacy and data-protection laws typically require organizations to implement appropriate safeguards to protect personal information across its lifecycle, including collection, storage, processing, sharing, and disposal. In cybersecurity governance documentation, this obligation is often expressed through requirements to maintain confidentiality and integrity of personal data, limit access based on business need, and ensure accountability through logging, monitoring, and audits.

Demonstrating protection of personal data generally includes having a documented data classification scheme, clearly defined lawful purposes for processing, retention limits, and secure handling procedures. Technical controls commonly expected include strong authentication, least privilege and role-based access control, encryption for data at rest and in transit, secure key management, endpoint and server hardening, vulnerability management, and continuous monitoring for suspicious activity. Operational capabilities such as incident response, breach detection, and timely notification processes are also emphasized because regulators expect organizations to manage and report material data exposures appropriately.

While protecting applications, intellectual property, and ensuring continuity are important security objectives, they are not the primary focus of many cybersecurity regulations in the same consistent way as personal data protection. Therefore, the best answer is personal data of customers and employees.

Question 4

Question Type: MultipleChoice

If a threat is expected to have a serious adverse effect, Based on NIST SP 800-30 it would be rated with a severity level of:

Options:

- A- moderate.
- B- severe.
- C- severely low.
- D- very severe.

Answer:

A

Explanation:

NIST SP 800-30 Rev. 1 defines qualitative risk severity levels using consistent impact language. In its assessment scale, "Moderate" is explicitly tied to events that can be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

A "serious adverse effect" is described as outcomes such as a significant degradation in mission capability where the organization can still perform its primary functions but with significantly reduced effectiveness, significant damage to organizational assets, significant financial loss, or significant harm to individuals that does not involve loss of life or life-threatening injuries. This phrasing is used to distinguish "Moderate" from "Low" (limited adverse effect) and from "High" (severe or catastrophic adverse effect).

This classification matters in enterprise risk because it drives prioritization and control selection. A "Moderate" rating typically triggers stronger treatment actions than "Low," such as tighter access controls, enhanced monitoring, more frequent vulnerability remediation, stronger configuration management, and improved incident response readiness. It also helps leaders compare risks consistently across systems and business processes by anchoring severity to clear operational and harm-based criteria rather than subjective judgment.

Question 5

Question Type: MultipleChoice

Controls that are put in place to address specific risks may include:

Options:

- A- only initial reviews.
- B- technology or process solutions.
- C- partial coverage of one or more risks.
- D- coverage for partial extent and scope of the risk.

Answer:

B

Explanation:

Cybersecurity controls are the safeguards an organization implements to reduce risk to an acceptable level. In standard risk-management language, a control is not limited to a one-time review; it is an ongoing capability that is designed, implemented, and operated to prevent, detect, or correct unwanted events. That capability is typically delivered through technology solutions (technical controls) and process solutions (administrative or procedural controls), which is why option B is correct.

Technology controls include items like firewalls, endpoint protection, encryption, multifactor authentication, logging and monitoring, vulnerability scanning, secure configuration baselines, and data-loss prevention. These controls directly enforce security requirements through system behavior and automation, helping reduce the likelihood or impact of threats.

Process controls include policies, standards, access approval workflows, segregation of duties, change management, secure development practices, incident response playbooks, training, and periodic access recertification. These ensure people consistently perform security-critical tasks correctly and create accountability and repeatability.

Options C and D describe possible outcomes or limitations (controls may not fully eliminate risk and may only mitigate part of it), but they are not what controls include. Option A is incorrect because "only initial reviews" are insufficient; reviews can be a component of a control, but effective controls require sustained operation, evidence, and reassessment as systems, threats, and business needs change.

Question 6

Question Type: MultipleChoice

Analyst B has discovered multiple attempts from unauthorized users to access confidential data. This is most likely?

Options:

- A- Admin
- B- Hacker
- C- User
- D- IT Support

Answer:

B

Explanation:

Multiple attempts by unauthorized users to access confidential data most closely aligns with activity from a hacker, meaning an unauthorized actor attempting to gain access to systems or information. Cybersecurity operations commonly observe this pattern as repeated login failures, password-spraying, credential-stuffing, brute-force attempts, repeated probing of restricted endpoints, or abnormal access requests against protected repositories. While "user" is too generic and could include authorized individuals, the question explicitly states "unauthorized users," pointing to malicious or illegitimate actors. "Admin" and "IT Support" are roles typically associated with legitimate privileged access and operational troubleshooting; repeated unauthorized access attempts from those roles would be atypical and would still represent compromise or misuse rather than normal operations. Cybersecurity documentation often classifies these attempts as indicators of malicious intent and potential precursor events to a breach. Controls recommended to counter such activity include strong authentication (multi-factor authentication), account lockout and throttling policies, anomaly detection, IP reputation filtering, conditional access, least privilege, and monitoring of authentication logs for patterns across accounts and geographies. The key distinction is that repeated unauthorized attempts represent hostile behavior by an external or rogue actor, which is best described as a hacker in the provided options.

Question 7

Question Type: MultipleChoice

Where SaaS is the delivery of a software service, what service does PaaS provide?

Options:

- A- Load Balancers
- B- Storage
- C- Subscriptions
- D- Operating System

Answer:

D

Explanation:

Cloud service models are commonly described as stacked layers of responsibility. Software as a Service delivers a complete application to the customer, while the provider manages the underlying platform and infrastructure. Platform as a Service sits one level below SaaS: it provides the managed platform needed to build, deploy, and run applications without the customer having to manage the underlying servers and most core system software.

A defining feature of PaaS is that the provider supplies and manages key platform components such as the operating system, runtime environment, middleware, web/application servers, and often supporting services like managed databases, messaging, scaling, and patching of the platform layer. The customer typically remains responsible for their application code, configuration, identities and access in the application, data classification and protection choices, and secure development practices. This shared responsibility model is central in cybersecurity guidance because it determines which security controls the provider enforces by default and which controls the customer must implement.

Given the answer options, Operating System is the best match because it is a core part of the platform layer that PaaS customers generally do not manage directly. Load balancers and storage can be consumed in multiple models, including IaaS and PaaS, and subscriptions describe a billing approach, not the technical service layer. Therefore, option D correctly reflects what PaaS provides compared to SaaS.

Bottom of Form

To Get Premium Files for IIBA-CCA Visit

<https://www.p2pexams.com/products/iiba-cca>

For More Free Questions Visit

<https://www.p2pexams.com/iiba/pdf/iiba-cca>

20%
DISCOUNT

P2P
exams