EXAMS 4 SUCCESS

IIBA

IIBA-CCA

Questions & Answers

Certificate in Cybersecurity Analysis (CCA)

(Demo Version - Limited Content)

Version: 4.0

Question: 1

There are three states in which data can exist:

A. at dead, in action, in use.

B. at dormant, in mobile, in use.

C. at sleep, in awake, in use.

D. at rest, in transit, in use.

Answer: D

Explanation:

Data is commonly categorized into three states because the threats and protections change depending on where the data is and what is happening to it. Data at rest is stored on a device or system, such as databases, file shares, endpoints, backups, and cloud storage. The main risks are unauthorized access, theft of storage media, misconfigured permissions, and improper disposal. Controls typically include strong access control, encryption at rest with sound key management, secure configuration and hardening, segmentation, and resilient backup protections including restricted access and immutability.

Data in transit is data moving between systems, such as client-to-server traffic, service-to-service connections, API calls, and email routing. The primary risks are interception, alteration, and impersonation through man-in-the-middle techniques. Standard controls include transport encryption (such as TLS), strong authentication and certificate validation, secure network architecture, and monitoring for anomalous connections or data flows.

Data in use is actively processed in memory by applications and users, for example when a document

is opened, a record is processed by an application, or data is displayed to a user. This state is challenging because data may be decrypted for processing. Controls include least privilege, strong authentication and session management, endpoint protection, application security controls, and secure development practices, with hardware-backed isolation when required.

Question: 2

Violations of the EU's General Data Protection Regulations GDPR can result in:

A. mandatory upgrades of the security infrastructure.

B. fines of €20 million or 4% of annual turnover, whichever is less.

C. fines of €20 million or 4% of annual turnover, whichever is greater.

D. a complete audit of the enterprise's security processes.

Answer: C

Explanation:

The GDPR establishes a regulatory penalty framework intended to make privacy and data-protection obligations enforceable across organizations of any size. Under GDPR, the most severe administrative fines can reach up to €20 million or up to 4% of the organization's total worldwide annual turnover of the preceding financial year, whichever is higher. That "whichever is greater" clause is critical: it prevents large enterprises from treating privacy violations as a minor cost of doing business and ensures the sanction can scale with the organization's economic size and risk impact.

Cybersecurity governance and risk documents typically emphasize GDPR as a driver for enterprise risk management because the consequences extend beyond monetary fines. A confirmed violation often triggers regulatory investigations, mandatory corrective actions, and potential restrictions on processing activities. Organizations may also face indirect impacts such as breach notification costs, legal claims from affected individuals, reputational harm, loss of customer trust, and increased oversight by regulators and auditors.

From a controls perspective, GDPR penalties reinforce the need for strong security and privacy-by-design practices: data minimization, lawful processing, documented purposes, retention controls, encryption where appropriate, access control and least privilege, monitoring and incident response readiness, and evidence-based accountability through policies, records, and audit trails. Selecting option C correctly reflects GDPR's maximum fine structure and its risk-based deterrence model.

Question: 3

What privacy legislation governs the use of healthcare data in the United States?

A. Privacy Act

B. PIPEDA

C. HIPAA

D. PCI-DSS

Answer: C

Explanation:

In the United States, HIPAA, the Health Insurance Portability and Accountability Act, is the primary federal framework that governs how certain healthcare information must be protected and used. In cybersecurity and compliance documentation, HIPAA is most often discussed through its implementing rules, especially the Privacy Rule and the Security Rule. The Privacy Rule establishes when protected health information may be used or disclosed and grants individuals rights over their health information. The Security Rule focuses specifically on safeguarding electronic protected health information by requiring administrative, physical, and technical safeguards.

From a security controls perspective, HIPAA-driven programs typically include risk analysis and risk management, policies and workforce training, access controls based on least privilege, unique user identification, authentication controls, audit logging, integrity protections, transmission security such as encryption for data in transit, and contingency planning such as backups and disaster recovery. HIPAA also expects organizations to manage third-party risk through appropriate agreements and oversight when vendors handle protected health information.

The other options do not fit the question. The Privacy Act generally applies to U.S. federal agencies' handling of personal records, PIPEDA is a Canadian privacy law, and PCI-DSS is an industry security standard focused on payment card data rather than healthcare data. Therefore, HIPAA is the correct legislation for U.S. healthcare data protection requirements.

Question: 4

Which of the following should be addressed by functional security requirements?

A. System reliability

B. User privileges

C. Identified vulnerabilities

D. Performance and stability

Answer: B

Explanation:

Functional security requirements define what security capabilities a system must provide to protect information and enforce policy. They describe required security functions such as identification and authentication, authorization, role-based access control, privilege management, session handling, auditing/logging, segregation of duties, and account lifecycle processes. Because of this, user privileges are a direct and core concern of functional security requirements: the system must support controlling who can access what, under which conditions, and with what level of permission.

In cybersecurity requirement documentation, “privileges” include permission assignment (roles, groups, entitlements), enforcement of least privilege, privileged access restrictions, elevation workflows, administrative boundaries, and the ability to review and revoke permissions. These are functional because they require specific system behaviors and features—for example, the ability to define roles, prevent unauthorized actions, log privileged activities, and enforce timeouts or re-authentication for sensitive operations.

The other options are typically classified differently. System reliability and performance/stability are generally non-functional requirements (quality attributes) describing service levels, resilience, and operational characteristics rather than security functions. Identified vulnerabilities are findings from assessments that drive remediation work and risk treatment; they inform security improvements but are not themselves functional requirements. Therefore, the option best aligned with functional security requirements is user privileges.

Question: 5

Which of the following terms represents an accidental exploitation of a vulnerability?

A. Threat

B. Agent

C. Event

D. Response

Answer: C

Explanation:

In cybersecurity risk terminology, an event is an observable occurrence that can affect systems, services, or data. An event may be benign, harmful, intentional, or accidental. When a vulnerability

is exploited accidentally—for example, a user unintentionally triggers a software flaw, a misconfiguration causes unintended exposure, or a system process mishandles input and causes data corruption—the occurrence is best categorized as an event. Cybersecurity documentation often distinguishes between the possibility of harm and the actual occurrence of a harmful condition. A threat is the potential for an unwanted incident, such as an actor or circumstance that could exploit a vulnerability. A threat does not require that exploitation actually happens; it describes risk potential. An agent is the entity that acts (such as a person, malware, or process) and may be malicious or non-malicious, but “agent” is not the term for the occurrence itself. A response refers to the actions taken after detection, such as containment, eradication, recovery, and lessons learned; it is part of incident handling, not the accidental exploitation.

Therefore, the term that represents the actual accidental exploitation occurrence is event, because it captures the real-world happening that may trigger alerts, investigations, and potentially incident response activities if impact is significant.

EXAMS 4 SUCCESS

Thank you for trying

Our IIBA-CCA Exam Dumps PDF Demo

Try IIBA-CCA practice question

If you want to try IIBA-CCA Exam Practice Test Questions So go to below link and try it!

https://www.exams4success.com/iiba-cca/practice-questions