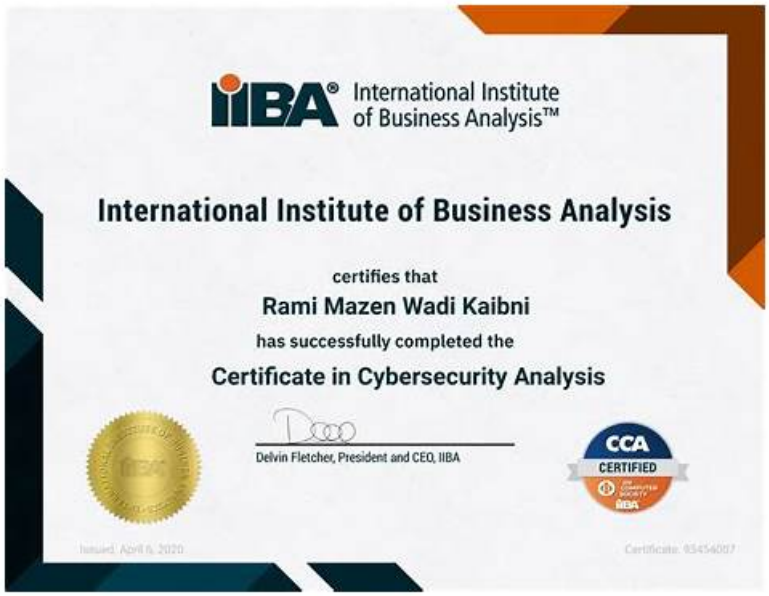
# Pass Guaranteed Quiz IIBA - IIBA-CCA - Professional Valid Certificate in Cybersecurity Analysis Test Dumps




What's more, part of that Free4Torrent IIBA-CCA dumps now are free: https://drive.google.com/open?id=195_0ij6iAqQl9BfcgjXxlsEtgcoIzoOI

Attending Free4Torrent, you will have best exam dumps for the certification of IIBA-CCA exam tests. We offer you the most accurate IIBA-CCA exam answers that will be your key to pass the certification exam in your first try. There are the best preparation materials for your IIBA-CCA Practice Test in our website to guarantee your success in a short time. Please totally trust the accuracy of questions and answers.

## IIBA IIBA-CCA Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Requirements Analysis and Design Definition: This domain involves analyzing, structuring, and specifying cybersecurity requirements in detail, and defining solution designs that address security needs while meeting stakeholder and organizational expectations. |
| Topic 2 | • Business Analysis Planning and Monitoring: This domain covers how to plan and oversee business analysis activities within a cybersecurity context, including defining approaches, stakeholder engagement plans, and governance of BA work throughout the project lifecycle. |
| Topic 3 | • Strategy Analysis: This domain covers assessing the current state of an organization's cybersecurity posture, identifying gaps and risks, and defining a future state and change strategy that aligns security needs with business objectives. |
| Topic 4 | • Solution Evaluation: This domain focuses on assessing cybersecurity solutions and their performance against defined requirements, identifying any gaps or limitations, and recommending improvements or corrective actions to maximize solution value. |

**>> Valid IIBA-CCA Test Dumps <<**

## IIBA-CCA Reliable Braindumps Ebook | IIBA-CCA Minimum Pass Score

If you are willing to clear exam successfully, you need to not only read books and study materials but also purchase IIBA IIBA-CCA reliable exam cram for well-directed review which will make you half the work with double results. You can find three versions for each exam: PDF version, Software version and APP version. You can choose one or more versions of IIBA-CCA Reliable Exam Cram based on your studying methods and habits.

## IIBA Certificate in Cybersecurity Analysis Sample Questions (Q45-Q50):

**NEW QUESTION # 45**
How is a risk score calculated?

- A. Based on past experience regarding the risk
- B. Based on the combination of probability and impact
- C. Based on an assessment of threats by the cyber security team
- D. Based on the confidentiality, integrity, and availability characteristics of the system

**Answer: B**

Explanation:
A risk score is commonly calculated by combining two core factors: how likely a risk scenario is to occur and how severe the consequences would be if it did occur. This is often described in cybersecurity risk documentation as likelihood times impact, or as a structured mapping using a risk matrix. Probability or likelihood reflects the chance that a threat event will exploit a vulnerability under current conditions. It may consider elements such as threat activity, exposure, ease of exploitation, control strength, and historical incident patterns. Impact reflects the magnitude of harm to the organization, usually measured across business disruption, financial loss, legal or regulatory exposure, reputational damage, and harm to confidentiality, integrity, or availability.
While confidentiality, integrity, and availability are essential for understanding what matters and can influence impact ratings, they are typically inputs into impact determination rather than the full scoring method by themselves. Past experience and expert threat assessment can inform likelihood estimates, but they are not the standard calculation model on their own. The key concept is that risk must reflect both chance and consequence; a highly impactful event with very low likelihood may be scored similarly to a moderate impact event with high likelihood depending on the organization's methodology.
Therefore, the most accurate description of how a risk score is calculated is the combination of probability and impact, enabling prioritization and consistent risk treatment decisions.

**NEW QUESTION # 46**
Violations of the EU's General Data Protection Regulations GDPR can result in:

- A. fines of €20 million or 4% of annual turnover, whichever is greater.
- B. fines of €20 million or 4% of annual turnover, whichever is less.
- C. a complete audit of the enterprise's security processes.
- D. mandatory upgrades of the security infrastructure.

**Answer: A**

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.

**NEW QUESTION # 47**
What stage of incident management would "strengthen the security from lessons learned" fall into?

- A. Recovery
- B. Detection
- C. Remediation
- D. Response

**Answer: C**

Explanation:
"Strengthen the security from lessons learned" fits the remediation stage because it focuses on eliminating root causes and improving controls so the same incident is less likely to recur. In incident management lifecycles, response is about immediate actions to contain and manage the incident (triage, containment, eradication actions in progress, communications, and preserving evidence). Detection is the identification and confirmation stage (alerts, analysis, validation, and initial classification). Recovery is restoring services to normal operation and verifying stability, including bringing systems back online, validating data integrity, and meeting recovery objectives.
After the environment is stable, organizations conduct a post-incident review and then implement corrective and preventive actions. That work is remediation: closing exploited vulnerabilities, hardening configurations, rotating credentials and keys, tightening access and privileged account controls, improving monitoring and logging coverage, updating firewall rules or segmentation, refining secure development practices, and correcting process gaps such as weak change management or incomplete asset inventory. Remediation also includes updating policies and playbooks, enhancing detection rules based on observed attacker techniques, and training targeted groups if human factors contributed.
Cybersecurity guidance emphasizes documenting lessons learned, assigning owners and deadlines, validating fixes, and tracking completion because "lessons learned" without implemented change does not reduce risk. The defining characteristic is durable improvement to the control environment, which is why this activity belongs to remediation rather than response, detection, or recovery.

**NEW QUESTION # 48**
Compliance with regulations is generally demonstrated through:

- A. independent audits of systems and security procedures.
- B. extensive QA testing prior to system implementation.
- C. review of security requirements by senior executives and/or the Board.
- D. penetration testing by ethical hackers.

**Answer: A**

Explanation:
Regulatory compliance is generally demonstrated through independent audits because regulators, customers, and partners typically require objective evidence that required controls exist and operate effectively. An independent audit is performed by a qualified party that is not responsible for running the controls being assessed, which strengthens credibility and reduces conflicts of interest. Cybersecurity and governance documents describe audits as a formal method to verify compliance against defined criteria such as laws, regulations, contractual obligations, or control frameworks. Auditors review policies and procedures, inspect system configurations, sample access and change records, evaluate logging and monitoring, test incident response evidence, and validate that controls are consistently performed over time. The outcome is usually a report, attestation, or findings with remediation plans-artifacts commonly used to prove compliance.
A Board or executive review supports governance and oversight, but it does not, by itself, provide independent verification that controls are functioning. QA testing focuses on product quality and functional correctness; it may include security testing but does not typically satisfy regulatory evidence requirements for ongoing operational controls. Penetration testing is valuable for identifying exploitable weaknesses, yet it is a point-in-time technical exercise and does not comprehensively demonstrate compliance with procedural, administrative, and operational requirements such as access governance, retention, training, vendor oversight, and continuous monitoring. Therefore, independent audits are the standard mechanism to demonstrate compliance in a defensible, repeatable way.

**NEW QUESTION # 49**
Which of the following terms represents an accidental exploitation of a vulnerability?

- A. Agent

- B. Event
- C. Response
- D. Threat

**Answer: B**

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.

**NEW QUESTION # 50**
.....

id=195_0ij6iAqQl9BfcgjXxlsEtgcoIzoOI