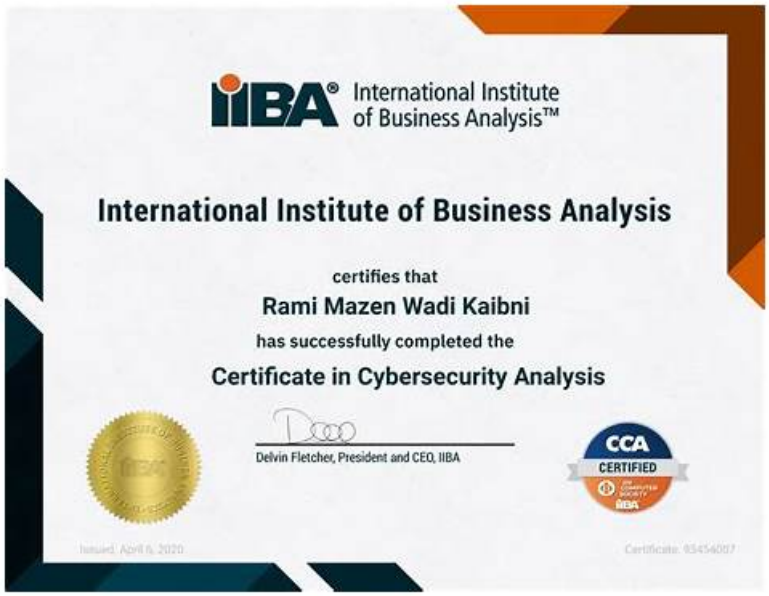
IIBA - IIBA-CCA - High Pass-Rate Certificate in Cybersecurity Analysis Latest Test Questions



DOWNLOAD the newest TestPDF IIBA-CCA PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1I8SxOzcfzhw4ULLuTwwPXa9bL2dp3yfK

Our IIBA-CCA learn materials can provide a good foundation for you to achieve your goal. A good job requires good skills, and the most intuitive way to measure your ability is how many qualifications you have passed and how many qualifications you have. With a qualification, you are qualified to do this professional job. Our IIBA-CCA Certification material is such a powerful platform, it can let you successfully obtain the IIBA-CCA certificate, from now on your life is like sailing, smooth sailing.

IIBA IIBA-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
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	• 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 5	• Elicitation and Collaboration: This domain focuses on techniques for gathering cybersecurity-related requirements and information from stakeholders, as well as fostering effective communication and collaboration among all parties involved.

>> IIBA-CCA Latest Test Questions <<

Pass Guaranteed Quiz IIBA-CCA - Accurate Certificate in Cybersecurity Analysis Latest Test Questions

TestPDF IIBA-CCA valid training material is the efforts of our professional experts. They edit and compile the IIBA-CCA questions and answers using their professional technology and hands-on experience. So if you want to pass with 100% guarantee, IIBA-CCA vlid exam files will give you security and high scores. You will complete your IIBA IIBA-CCA exam preparation in a short time and attend the actual test with comfortable mood.

IIBA Certificate in Cybersecurity Analysis Sample Questions (Q13-Q18):

NEW QUESTION # 13
A significant benefit of role-based access is that it:

- A. ensures that employee accounts will be shut down on departure or role change.
- B. simplifies the assignment of correct access levels to a user based on the work they will perform.
- C. ensures that tasks and associated privileges for a specific business process are disseminated among multiple users.
- D. makes it easier to audit and verify data access.

Answer: B

Explanation:
Role-based access control assigns permissions to defined roles that reflect job functions, and users receive access by being placed into the appropriate role. The major operational and security benefit is that it simplifies and standardizes access provisioning. Instead of granting permissions individually to each user, administrators manage a smaller, controlled set of roles such as Accounts Payable Clerk, HR Specialist, or Application Administrator. When a new employee joins or changes responsibilities, access can be adjusted quickly and consistently by changing role membership. This reduces manual errors, limits over-provisioning, and helps enforce least privilege because each role is designed to include only the permissions required for that function.
RBAC also improves governance by making access decisions more repeatable and policy-driven. Security and compliance teams can review roles, validate that each role's permissions match business needs, and require approvals for changes to role definitions. This approach supports segregation of duties by separating conflicting capabilities into different roles, which lowers fraud and misuse risk.
Option B is a real advantage of RBAC, but it is typically a secondary outcome of having structured roles rather than the primary "significant benefit" emphasized in access-control design. Option C relates to identity lifecycle processes such as deprovisioning, which can be integrated with RBAC but is not guaranteed by RBAC alone. Option D describes distributing tasks among multiple users, which is more aligned with segregation of duties design, not the core benefit of RBAC.

NEW QUESTION # 14
What is whitelisting in the context of network security?

- A. Explicitly allowing identified people, groups, or services access to a particular privilege, service, or recognition
- B. Denying access to applications that have been determined to be malicious
- C. Running software to identify any malware present on a computer system
- D. Grouping assets together based on common security requirements, and placing each group into an isolated network zone

Answer: A

Explanation:
Whitelisting, often called an "allow list," is a security approach where access is granted only to explicitly approved identities, services, applications, IP addresses, domains, or network flows. In network security, this means the default stance is "deny by default," and only pre-authorized entities are allowed to communicate or use specific resources. Option C matches this definition because it describes the core idea: explicitly permitting known, approved subjects (people, groups, service accounts, systems) to access a defined privilege or service.
Cybersecurity documents emphasize whitelisting as a strong risk-reduction technique because it constrains the attack surface. Instead of trying to block every bad thing (which is difficult due to evolving threats), whitelisting focuses on allowing only what is required for business operations. Examples include firewall rules that only permit specific source IPs to reach an admin interface, network segmentation policies that allow only required ports between zones, and application whitelisting that permits only approved executables to run. When implemented correctly, it reduces lateral movement opportunities, limits command-and-control traffic, and prevents unauthorized tools from executing.
Whitelisting is different from segmentation (option A), which is about isolating zones based on security needs, and different from

blacklisting (option B), which blocks known-bad items. It is also not malware scanning (option D), which detects malicious code after it appears. Whitelisting aligns with least privilege and zero trust principles by tightly controlling what is allowed.

NEW QUESTION # 15
How should categorization information be used in business impact analysis?

- A. To identify discrepancies between the security categorization and the expected business impact
- B. To ensure that systems are designed to support the appropriate security categorization
- C. To determine the time and effort required for business impact assessment
- D. To assess whether information should be shared with other systems

Answer: A

Explanation:
Security categorization (commonly based on confidentiality, integrity, and availability impact levels) is meant to reflect the level of harm that would occur if an information type or system is compromised. A business impact analysis, on the other hand, examines the operational and organizational consequences of disruptions or failures-such as loss of revenue, inability to deliver critical services, legal or regulatory exposure, reputational harm, and impacts to customers or individuals. Because these two activities look at impact from different but related perspectives, categorization information should be used during the BIA to confirm that the stated security categorization truly matches real business consequences.
Using categorization as an input helps analysts validate assumptions about criticality, sensitivity, and tolerance for downtime. If the BIA shows that outages or data compromise would produce greater harm than the existing categorization implies, that discrepancy signals under-classification and insufficient controls. Conversely, if the BIA demonstrates limited impact, it may indicate over-classification, potentially driving unnecessary cost and operational burden. Identifying these mismatches early supports better risk decisions, prioritization of recovery objectives, and selection of controls proportionate to actual impact.
The other options describe activities that may occur in architecture, governance, or project planning, but they are not the primary purpose of using categorization information in a BIA. The key value is reconciliation: aligning security impact levels with verified business impact.

NEW QUESTION # 16
What stage of incident management would "strengthen the security from lessons learned" fall into?

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

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 # 17
What privacy legislation governs the use of healthcare data in the United States?

- A. Privacy Act
- B. PCI-DSS
- C. HIPAA
- D. PIPEDA

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.

NEW QUESTION # 18
.....

www.exam4labs.com □✔□ will open immediately □New IIBA-CCA Mock Exam

- thebookmarkplaza.com, nanavguy454042.dailyblogzz.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, kalepctc042405.blog-kids.com, www.stes.tyc.edu.tw, doctorbookmark.com, www.stes.tyc.edu.tw, emiliachtf255388.blogsuperapp.com, www.stes.tyc.edu.tw, kallumlcfw872775.slypage.com, Disposable vapes

P.S. Free 2026 IIBA IIBA-CCA dumps are available on Google Drive shared by TestPDF: https://drive.google.com/open?id=1I8SxOzcfzhw4ULLuTwwPXa9bL2dp3yfK