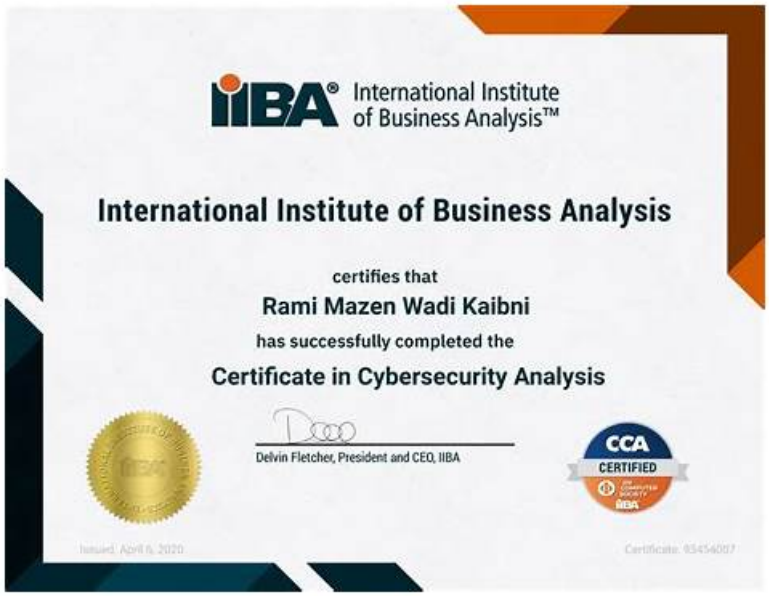
Quiz High Hit-Rate IIBA - IIBA-CCA - Verified Certificate in Cybersecurity Analysis Answers



What's more, part of that PassSureExam IIBA-CCA dumps now are free: https://drive.google.com/open?id=1opT8ddfvpiiSrT3srirRBrgquFrnXfpp

PassSureExam is a wonderful study platform that contains our hearty wish for you to pass the exam by our IIBA-CCA exam materials. So our responsible behaviors are our instinct aim and tenet. By devoting in this area so many years, we are omnipotent to solve the problems about the IIBA-CCA learning questions with stalwart confidence. we can claim that only studing our IIBA-CCA study guide for 20 to 30 hours, then you will pass the exam for sure.

IIBA IIBA-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• Requirements Life Cycle Management: This domain addresses how to manage and maintain cybersecurity requirements from initial identification through to solution implementation, including tracing, prioritizing, and controlling changes to requirements.
Topic 2	• 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.
Topic 3	• 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.

>> Verified IIBA-CCA Answers <<

Dumps IIBA IIBA-CCA Free, IIBA-CCA New Learning Materials

Our IIBA-CCA practice exam simulator mirrors the IIBA-CCA exam experience, so you know what to anticipate on IIBA-CCA exam day. Our IIBA IIBA-CCA features various question styles and levels, so you can customize your IIBA-CCA exam questions preparation to meet your needs.

IIBA Certificate in Cybersecurity Analysis Sample Questions (Q69-Q74):

NEW QUESTION # 69
If a Business Analyst is asked to document the current state of the organization's web-based business environment, and recommend where cost savings could be realized, what risk factor must be included in the analysis?

- A. Threat Likelihood
- B. Application Vulnerabilities
- C. Organizational Risk Tolerance
- D. Impact Severity

Answer: B

Explanation:
When analyzing a web-based business environment for potential cost savings, the Business Analyst must account for application vulnerabilities because they directly affect the organization's exposure to cyber attack and the true cost of operating a system. Vulnerabilities are weaknesses in application code, configuration, components, or dependencies that can be exploited to compromise confidentiality, integrity, or availability. In web environments, common examples include insecure authentication, injection flaws, broken access control, misconfigurations, outdated libraries, and weak session management.
Cost-saving recommendations frequently involve consolidating platforms, reducing tooling, lowering support effort, retiring controls, delaying upgrades, or moving to shared services. Without including known or likely vulnerabilities, the analysis can unintentionally recommend changes that reduce preventive and detective capability, increase attack surface, or extend the time vulnerabilities remain unpatched. Cybersecurity governance guidance emphasizes that technology rationalization must consider security posture: vulnerable applications often require additional controls (patching cadence, WAF rules, monitoring, code fixes, penetration testing, secure SDLC work) that carry ongoing cost. These costs are part of the system's "total cost of ownership" and should be weighed against proposed savings.
While impact severity and threat likelihood are important for overall risk scoring, the question asks what risk factor must be included when documenting the current state of a web-based environment. The most essential factor that ties directly to the environment's condition and drives remediation cost and exposure is application vulnerabilities.

NEW QUESTION # 70
Which of the following should be addressed by functional security requirements?

- A. Identified vulnerabilities
- B. Performance and stability
- C. System reliability
- D. User privileges

Answer: D

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.

NEW QUESTION # 71
The main phases of incident management are:

- A. reporting, investigation, assessment, corrective actions, review.
- B. assess, investigate, report, respond, legal compliance.

- C. initiation, planning, action, closing.
- D. awareness, interest, desire, action.

Answer: A

Explanation:
Incident management is a structured operational process used to ensure security issues are handled consistently, evidence is preserved, impact is reduced, and improvements are implemented to prevent recurrence. The phases listed in option B match how incident management is commonly documented in operational security programs.
Reporting is the entry point: users, monitoring tools, and service desks raise alerts or tickets, capturing what happened, when, and initial impact. Clear reporting channels and defined severity criteria ensure incidents are escalated quickly and handled by the right teams. Investigation follows, focusing on fact-finding and evidence collection such as logs, endpoint telemetry, network traces, and user statements. Assessment determines scope, business impact, affected assets and data, and the likelihood of continuing compromise. This step drives prioritization and selects the appropriate handling path.
Corrective actions implement containment, eradication, and recovery activities, such as isolating hosts, disabling compromised accounts, applying patches, rotating credentials, restoring from backups, and validating system integrity. Corrective actions also include communications, documentation, and coordination with legal, privacy, and business stakeholders when required. Finally, review is the lessons-learned phase that updates playbooks, improves detections, closes control gaps, and ensures root causes are addressed through durable fixes rather than temporary workarounds.
The other options do not represent standard incident management phases: A is a marketing model, while C and D are incomplete or mis-ordered compared to established incident management lifecycle documentation.

NEW QUESTION # 72
Which capability would a solution option need to demonstrate in order to satisfy Logging Requirements?

- A. Integrates with Risk Logging software
- B. Offers both on-premise and as-a-service delivery options
- C. Facilitates Single Sign-On
- D. Records information about user access and actions in the system

Answer: D

Explanation:
Logging requirements in cybersecurity focus on ensuring the system can produce reliable, actionable records that support detection, investigation, compliance, and accountability. The most fundamental capability is the ability to record information about user access and actions within the system. This includes authentication events such as logon success or failure, logoff, session creation, and privilege elevation; authorization decisions such as access granted or denied; and security-relevant actions such as viewing, creating, modifying, deleting, exporting, or transmitting sensitive data. Good security logging also captures context like timestamp synchronization, user or service identity, source device or IP, target resource, action performed, and outcome.
This capability supports multiple operational needs. Security monitoring teams rely on logs to identify anomalies like repeated failed logins, unusual access times, access from unexpected locations, or high-risk administrative changes. Incident responders need logs to reconstruct timelines, confirm scope, and preserve evidence. Auditors and compliance teams require logs to demonstrate control effectiveness, segregation of duties, and traceability of changes.
The other options are not sufficient to satisfy logging requirements. Single sign-on can simplify authentication but does not guarantee application-level activity logging. Integration with specialized tools may be useful, but the solution must first generate the required events. Deployment model options do not address whether the system can create detailed audit trails. Therefore, the required capability is recording user access and actions in the system.

NEW QUESTION # 73
Cybersecurity regulations typically require that enterprises demonstrate that they can protect:

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

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.

NEW QUESTION # 74
.....

Our IIBA IIBA-CCA practice exam software is the most impressive product to learn and practice. We have a team of professional software developers to ensure the software's productivity. After installation, IIBA IIBA-CCA Practice Exam software is used without an internet connection.