IIBA-CCA Latest Exam Materials, IIBA-CCA Latest Dumps Files

2026 Latest Lead2Passed IIBA-CCA PDF Dumps and IIBA-CCA Exam Engine Free Share: https://drive.google.com/open?id=1HfcDm_5vVeRVAXTEjmUEY18rlYgQJw7k

Our reliable IIBA-CCA question dumps are developed by our experts who have rich experience in the fields. Constant updating of the IIBA-CCA prep guide keeps the high accuracy of exam questions thus will help you get use the IIBA-CCA Exam quickly. During the exam, you would be familiar with the questions, which you have practiced in our IIBA-CCA question dumps. That's the reason why most of our customers always pass exam easily.

IIBA IIBA-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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.

>> IIBA-CCA Latest Exam Materials <<

100% Pass 2026 IIBA Unparalleled IIBA-CCA: Certificate in Cybersecurity Analysis Latest Exam Materials

Your privacy and personal right are protected by our company and corresponding laws and regulations on our IIBA-CCA study guide. Whether you are purchasing our IIBA-CCA training questions, installing or using them, we won't give away your information to other platforms, and the whole transaction process will be open and transparent. Therefore, let us be your long-term partner and we promise our IIBA-CCA Preparation exam won't let down.

IIBA Certificate in Cybersecurity Analysis Sample Questions (Q26-Q31):

NEW QUESTION # 26
The main phases of incident management are:

- A. initiation, planning, action, closing.
- B. awareness, interest, desire, action.
- C. assess, investigate, report, respond, legal compliance.
- D. reporting, investigation, assessment, corrective actions, review.

Answer: D

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 # 27
Which of the following is a cybersecurity risk that should be addressed by business analysis during solution development?

- A. Code may be implemented in ways that introduce new vulnerabilities
- B. QA may fail to identify all possible security vulnerabilities during system testing
- C. Project budgets may prevent developers from implementing the full set of security measures
- D. The solution may not be understood well enough to reliably identify security risks

Answer: D

Explanation:
Business analysis is responsible for ensuring the solution is correctly understood in terms of business purpose, process flows, data handling, user roles, integrations, and non-functional requirements such as security and privacy. If the solution is not understood well enough, security risks will be missed early, leading to gaps that are expensive and difficult to correct later. This is why option C is the best answer: inadequate understanding prevents reliable identification of threats, sensitive data paths, trust boundaries, and misuse cases during requirements and design stages.
Cybersecurity documents emphasize "security by design" and "shift-left" practices, meaning risks should be identified and addressed before build and test. Business analysis contributes by eliciting and documenting security requirements, clarifying data classification and retention needs, defining user access and privilege expectations, identifying regulatory and policy constraints, and ensuring interfaces and third-party dependencies are known and assessed. BA also supports threat modeling inputs by providing accurate context about actors, workflows, and data movement, which are essential for identifying where controls like authentication, authorization, logging, encryption, and validation must exist.
Other options align to different roles or stages: budgets are governance and project management constraints, QA limitations are testing risks, and coding-introduced vulnerabilities are primarily addressed through secure coding standards, code review, and developer practices. BA's key cybersecurity risk is incomplete understanding that prevents correct security requirements and risk identification.

NEW QUESTION # 28
An internet-based organization whose address is not known has attempted to acquire personal identification details such as usernames and passwords by creating a fake website. This is an example of?

- A. Ransomware
- B. Phishing
- C. Breach
- D. Threat

Answer: B

Explanation:
Creating a fake website to trick individuals into entering usernames and passwords is a classic example of phishing. Phishing is a social engineering technique where an attacker impersonates a trusted entity to deceive a victim into disclosing sensitive information (credentials, personal data, payment details) or taking an action that benefits the attacker (downloading malware, approving an MFA prompt, wiring funds). A counterfeit login page is commonly used in credential-harvesting campaigns: the victim believes they are authenticating to a legitimate service, but the credentials are captured by the attacker and later used for account takeover. This is not necessarily a breach yet because the question describes an attempt to acquire credentials; a breach would be confirmed unauthorized access or disclosure. While phishing is a kind of threat, "threat" is too broad compared to the specific described behavior. It is also not ransomware, which focuses on encrypting or locking data and demanding payment. Cybersecurity documentation emphasizes layered defenses against phishing: user awareness training, email and web filtering, domain and certificate validation, anti-spoofing controls, strong authentication (especially MFA resistant to prompt fatigue), password managers that reduce credential entry on lookalike domains, and monitoring for suspicious logins. Because the attack relies on deception through a fake website to steal credentials, the best match is phishing.

NEW QUESTION # 29
Compliance with regulations is generally demonstrated through:

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

Answer: B

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 # 30
The hash function supports data in transit by ensuring:

- A. a message was modified in transit.
- B. encrypted messages are not shared with another party.

- C. a public key is transitioned into a private key.
- D. validation that a message originated from a particular user.

Answer: A

Explanation:
A cryptographic hash function supports data in transit primarily by providing integrity assurance. When a sender computes a hash (digest) of a message and the receiver recomputes the hash after receipt, the two digests should match if the message arrived unchanged. If the message is altered in any way while traveling across the network-whether by an attacker, a faulty intermediary device, or transmission errors-the recomputed digest will differ from the original. This difference is the key signal that the message was modified in transit, which is what option B expresses. In practical secure-transport designs, hashes are typically combined with a secret key or digital signature so an attacker cannot simply modify the message and generate a new valid digest. Examples include HMAC for message authentication and digital signatures that hash the content and then sign the hash with a private key. These mechanisms provide integrity and, when keyed or signed, also provide authentication and non-repudiation properties.
Option A is more specifically about authentication of origin, which requires a keyed construction such as HMAC or a signature scheme; a plain hash alone cannot prove who sent the message. Option C is incorrect because keys are not "converted" from public to private. Option D relates to confidentiality, which is provided by encryption, not hashing. Therefore, the best answer is B because hashing enables detection of message modification during transit.

NEW QUESTION # 31
.....

id=1HfcDm_5vVeRVAXTEjmUEY18rlYgQJw7k