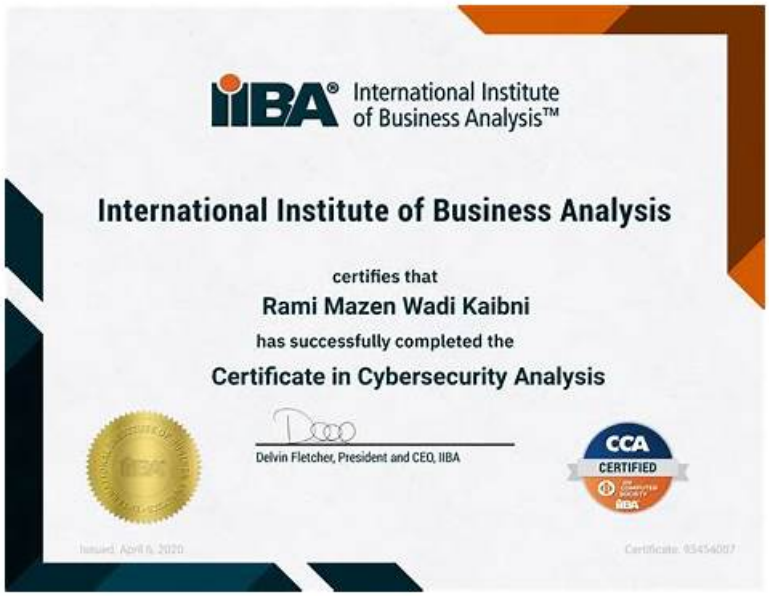
2026 IIBA-CCA Study Dumps - Trustable IIBA Certificate in Cybersecurity Analysis - 100% IIBA-CCA Correct Answers



P.S. Free & New IIBA-CCA dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1oVGNxZqG_g0KYqIPAjKsglqj9ztI1mbU

The development and progress of human civilization cannot be separated from the power of knowledge. You must learn practical knowledge to better adapt to the needs of social development. Now, our IIBA-CCA learning materials can meet your requirements. You will have good command knowledge with the help of our study materials. The certificate is of great value in the job market. Our IIBA-CCA Study Materials can exactly match your requirements and help you pass exams and obtain certificates. As you can see, our products are very popular in the market. Time and tides wait for no people.

You will be able to assess your shortcomings and improve gradually without having anything to lose in the actual IIBA IIBA-CCA exam. You will sit through mock exams and solve actual IIBA IIBA-CCA Dumps. In the end, you will get results that'll improve each time you progress and grasp the concepts of your syllabus.

>> IIBA-CCA Study Dumps <<

100% IIBA-CCA Correct Answers | Sample IIBA-CCA Questions Pdf

The trouble can test a person's character. A bad situation can show special integrity. When to face of a difficult time, only the bravest people could take it easy. Are you a brave person? If you did not do the best preparation for your IT certification exam, can you take it easy? Yes, of course. Because you have itPass4sure's IIBA IIBA-CCA Exam Training materials. As long as you have it, any examination do not will knock you down.

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	• 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	• 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.

IIBA Certificate in Cybersecurity Analysis Sample Questions (Q49-Q54):

NEW QUESTION # 49
What is risk mitigation?

- A. Eliminating the risk by stopping the activity which causes risk
- B. Documenting the risk in full and preparing a recovery plan
- C. Reducing the risk by implementing one or more countermeasures
- D. Purchasing insurance against a cybersecurity breach

Answer: C

Explanation:
Risk mitigation is the risk treatment approach focused on reducing risk to an acceptable level by lowering either the likelihood of a risk event, the impact of that event, or both. In cybersecurity risk management, mitigation is accomplished by implementing controls and countermeasures such as technical safeguards, process changes, and administrative measures. Examples include patching vulnerable systems, hardening configurations, enabling multi-factor authentication, applying least privilege, network segmentation, encryption, improved logging and monitoring, secure development practices, and user awareness training. Each of these actions reduces exposure or limits damage if an incident occurs.
The other options describe different risk treatment strategies, not mitigation. Purchasing insurance is generally considered risk transfer, where financial impact is shifted to a third party, but the underlying threat and vulnerability may still exist. Eliminating risk by stopping the risky activity is risk avoidance; it removes the exposure by discontinuing the process, system, or behavior causing the risk. Documenting the risk and preparing a recovery plan aligns more closely with risk acceptance combined with contingency planning or resilience planning; it acknowledges the risk and focuses on recovery rather than reducing the probability of occurrence. Therefore, the correct definition of risk mitigation is reducing the risk through implementing one or more countermeasures.

NEW QUESTION # 50
What is a Recovery Point Objective RPO?

- A. The maximum time a system may be out of service before a significant business impact occurs
- B. The point in time prior to the outage to which business and process data must be recovered
- C. The target time to restore systems to operational status following an outage
- D. The target time to restore a system without experiencing any significant business impact

Answer: B

Explanation:
A Recovery Point Objective defines the acceptable amount of data loss measured in time. It answers the question: "After an outage or disruptive event, how far back in time can we restore data and still meet business needs?" If the RPO is 4 hours, the organization is stating it can tolerate losing up to 4 hours of data changes, meaning backups, replication, journaling, or snapshots must be frequent enough to restore to a point no older than 4 hours before the incident. That is exactly what option A describes: the specific point in time prior to the outage to which data must be recovered.
RPO is often paired with Recovery Time Objective but they are not the same. RTO focuses on how quickly service must be restored, while RPO focuses on how much data the organization can afford to lose. Options B, C, and D all describe time-to-restore concepts, which align with RTO or related recovery targets rather than RPO.
In operational resilience and disaster recovery planning, RPO drives technical design choices: backup frequency, replication

methods, storage and retention strategies, and validation testing. Lower RPO values generally require more robust and often more expensive solutions, such as near-real-time replication and strong change capture controls. RPO also influences incident response and recovery procedures to ensure restoration steps reliably meet the agreed data-loss tolerance.
Top of Form

NEW QUESTION # 51
Separation of duties, as a security principle, is intended to:

- A. balance user workload.
- B. optimize security application performance.
- C. prevent fraud and error.
- D. ensure that all security systems are integrated.

Answer: C

Explanation:
Separation of duties is a foundational access-control and governance principle designed to reduce the likelihood of misuse, fraud, and significant mistakes by ensuring that no single individual can complete a critical process end-to-end without independent oversight. Cybersecurity and audit frameworks describe this as splitting high-risk activities into distinct roles so that one person's actions are checked or complemented by another person's authority. This limits both intentional abuse, such as unauthorized payments or data manipulation, and unintentional errors, such as misconfigurations or accidental deletion of important records.
In practice, separation of duties is implemented by defining roles and permissions so that incompatible functions are not assigned to the same account. Common examples include separating the ability to create a vendor from the ability to approve payments, separating software development from production deployment, and separating system administration from security monitoring or audit log management. This is reinforced through role-based access control, approval workflows, privileged access management, and periodic access reviews that detect conflicting entitlements and privilege creep.
The value of separation of duties is risk reduction through accountability and control. When actions require multiple parties or independent review, it becomes harder for a single compromised account or malicious insider to cause large harm without detection. It also improves reliability by introducing checkpoints that catch mistakes earlier. Therefore, the correct purpose is to prevent fraud and error.

NEW QUESTION # 52
What is whitelisting in the context of network security?

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

Answer: B

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 # 53
Public & Private key pairs are an example of what technology?

- A. IoT
- B. Network Segregation
- C. Virtual Private Network
- D. Encryption

Answer: D

Explanation:
Public and private key pairs are the foundation of asymmetric encryption, also called public key cryptography. In this model, each entity has two mathematically related keys: a public key that can be shared widely and a private key that must be kept secret. The keys are designed so that what one key does, only the other key can undo. This enables two core security functions used throughout cybersecurity architectures.
First, confidentiality: data encrypted with a recipient's public key can only be decrypted with the recipient's private key. This allows secure communication without having to share a secret key in advance, which is especially important on untrusted networks like the internet. Second, digital signatures: a sender can sign data with their private key, and anyone can verify the signature using the sender's public key. This provides authenticity (proof the sender possessed the private key), integrity (the data was not altered), and supports non-repudiation when combined with proper key custody and audit practices.
These mechanisms underpin widely used security controls such as TLS for secure web connections, secure email standards, code signing, and certificate-based authentication. A VPN may use public key cryptography during key exchange, but the key pair itself is specifically an encryption technology. IoT and network segregation are unrelated categories.

NEW QUESTION # 54
.....

adreahbcz896910.newsbloger.com, jessexgjl013566.dreamyblogs.com, trackbookmark.com, sirketlist.com, isocialfans.com, socialbuzzfeed.com, Disposable vapes

What's more, part of that itPass4sure IIBA-CCA dumps now are free: https://drive.google.com/open?id=1oVGNxZqG_g0KYqIPAjKsglqj9ztI1mbU