Certification IIBA IIBA-CCA Test Questions | Valid Braindumps IIBA-CCA Pdf

BTW, DOWNLOAD part of Pass4Test IIBA-CCA dumps from Cloud Storage: https://drive.google.com/open?id=1eLNwFV0nrhUFbs-1TOdqm7vximAJEq_4

Pass4Test has designed IIBA IIBA-CCA pdf dumps format that is easy to use. Anyone can download the IIBA IIBA-CCA pdf questions file and use it from any location or at any time. IIBA PDF Questions files can be used on laptops, tablets, and smartphones. Moreover, you will get actual IIBA IIBA-CCA Pdf Dumps file.

About the upcoming IIBA-CCA exam, do you have mastered the key parts which the exam will test up to now? Everyone is conscious of the importance and only the smart one with smart way can make it. When new changes or knowledge are updated, our experts add additive content into our IIBA-CCA latest material. They have always been in a trend of advancement. Admittedly, our IIBA-CCA Real Questions are your best choice. We also estimate the following trend of exam questions may appear in the next exam according to syllabus. So they are the newest and also the most trustworthy IIBA-CCA exam prep to obtain.

>> Certification IIBA IIBA-CCA Test Questions <<

For Quick Exam preparation download, the IIBA IIBA-CCA Exam dumps

Our IIBA-CCA training guide is not difficult for you. We have simplified all difficult knowledge. So you will enjoy learning our IIBA-CCA study quiz. During your practice of our IIBA-CCA exam materials, you will find that it is easy to make changes. In addition, our study materials will boost your confidence. You will be glad to witness your growth. Do not hesitate. Good opportunities will slip away if you stand still.

IIBA IIBA-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 5	• 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.

IIBA Certificate in Cybersecurity Analysis Sample Questions (Q72-Q77):

NEW QUESTION # 72
Which organizational resource category is known as "the first and last line of defense" from an attack?

- A. Classified Data
- B. Endpoint Devices
- C. Firewalls
- D. Employees

Answer: D

Explanation:
In cybersecurity guidance, employees are often described as the first and last line of defense because human actions influence nearly every stage of an attack. They are the first line since many threats begin with user interaction: phishing emails, malicious links, social engineering calls, unsafe file handling, weak passwords, and accidental disclosure of sensitive information. A well-trained user who recognizes suspicious requests, verifies identities, and reports anomalies can stop an incident before any technical control is even engaged.
Employees are also the last line because technical protections such as firewalls, filters, and endpoint tools are not perfect. Attackers routinely bypass or evade automated defenses using stolen credentials, living-off-the-land techniques, misconfigurations, or novel malware. When those controls fail, the organization still depends on people to apply secure behaviors: following least privilege, protecting credentials, using multifactor authentication correctly, confirming out-of-band requests for payments or data, and escalating unusual activity quickly. Incident response, containment, and recovery also depend on humans making correct decisions under pressure, following documented procedures, and communicating accurately.
Cybersecurity documents emphasize that a strong security culture, regular awareness training, role-based education, clear reporting channels, and consistent policy enforcement reduce human-enabled risk and turn employees into an effective security control rather than a vulnerability.

NEW QUESTION # 73
Protecting data at rest secures data that is:

- A. stored on any device or network.
- B. moving from network to network.
- C. less vulnerable to attack.
- D. moving from device to device.

Answer: A

Explanation:
Data at rest refers to information that is stored rather than actively moving across networks or being actively processed. This includes data saved on laptops and mobile devices, servers, databases, file shares, removable media, backup tapes, storage arrays, and cloud storage services. Because it sits in storage, the main risks involve unauthorized access (improper permissions, stolen credentials, insider misuse), theft or loss of devices/media, and misconfiguration (publicly exposed storage buckets, overly broad shared drives). Data at rest is also at risk when systems are decommissioned or storage is reused without secure wiping.
Cybersecurity documents emphasize protecting data at rest using layered controls. Encryption at rest ensures stored files or database records remain unreadable without the proper key, reducing impact if storage is stolen or accessed improperly. Strong access control and least privilege limit who can read or modify stored data, while segmentation and secure configuration reduce exposure pathways. Proper key management (separating keys from encrypted data, rotating keys, restricting key access) is critical so encryption meaningfully reduces risk. Additional controls include data classification and handling rules, secure backups (including immutable or protected backups), monitoring and audit logging for sensitive repositories, and secure disposal practices such as

cryptographic erase or verified wiping.
Options A and B describe data in transit, not at rest. Option D is incorrect because stored data is not automatically less vulnerable; it is often highly attractive to attackers, so it requires deliberate protection.

NEW QUESTION # 74
Separation of duties, as a security principle, is intended to:

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

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 # 75
In the OSI model for network communication, the Session Layer is responsible for:

- A. adding appropriate network addresses to packets.
- B. establishing a connection and terminating it when it is no longer needed.
- C. transmitting the data on the medium.
- D. presenting data to the receiver in a form that it recognizes.

Answer: B

Explanation:
The OSI Session Layer (Layer 5) is responsible for establishing, managing, and terminating sessions between communicating applications. A session is the logical dialogue that allows two endpoints to coordinate how communication starts, how it continues, and how it ends. This includes controlling the "conversation" state, such as who can transmit at what time, maintaining the session so it stays active, and closing it cleanly when it is no longer needed. Because of this, option A best matches the Session Layer's core responsibilities.
In contrast, presenting data to the receiver in a recognizable form is the job of the Presentation Layer (Layer 6), which deals with formatting, encoding, compression, and often cryptographic transformation concepts. Adding appropriate network addresses to packets aligns to the Network Layer (Layer 3), where logical addressing and routing decisions occur, typically associated with IP addressing. Transmitting the data on the medium is handled at the Physical Layer (Layer 1), which concerns signals, cabling, and the actual movement of bits.
From a cybersecurity perspective, session management is important because weaknesses can enable session hijacking, replay, or fixation, especially when session identifiers are predictable, not protected, or not properly invalidated. Controls commonly include strong authentication, secure session token generation, timeout and reauthentication rules, and proper session termination to reduce exposure.

NEW QUESTION # 76

Violations of the EU's General Data Protection Regulations GDPR can result in:

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

Answer: D

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 # 77
.....

Successful people are those who are willing to make efforts. If you have never experienced the wind and rain, you will never see the rainbow. Giving is proportional to the reward. Now, our IIBA-CCA study materials just need you spend less time, then your life will take place great changes. Maybe you think that our IIBA-CCA study materials cannot make a difference. But you must know that if you do not have a try, your life will never be improved. It is useless that you speak boast yourself but never act. Please muster up all your courage. No one will laugh at a hardworking person. Our IIBA-CCA Study Materials are your good study partner.

- lewisqmkc019546.ourcodeblog.com, zubairfalh086255.gynoblog.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, www.stes.tyc.edu.tw, www.mirscz.com, eliteglobinternships.com, thebookmarkage.com, iowa-bookmarks.com, elainexldz606868.iyublog.com, bookmarksaifi.com, Disposable vapes

P.S. Free & New IIBA-CCA dumps are available on Google Drive shared by Pass4Test: https://drive.google.com/open?id=1eLNwFV0nrhUFbs-1TOdqm7vximAJEq_4