IIBA-CCA New Braindumps Questions | IIBA-CCA Latest Exam Pass4sure

What's more, part of that GetValidTest IIBA-CCA dumps now are free: https://drive.google.com/open?id=1GK_fPVyhAbSYw0mvVJj_Ig9hfT3LV4I2

As an IT field top company IIBA certifications are verified as senior products expert standards. IIBA field reputation and products market share improve certification engine's high gold content. IIBA-CCA latest vce exam simulator can help you pass exam and get certification so that you can obtain senior position soon. Senior engineers with professional certification have 60% opportunities and 30% salary or so more than normal engineers.

IIBA IIBA-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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 New Braindumps Questions <<

IIBA-CCA Latest Exam Pass4sure & IIBA-CCA Exam Dumps

If you think it is an adventure for purchasing our IIBA IIBA-CCA braindump, life is also a great adventure. Before many successful people obtained achievements, they had a adventure experience. Moreover, the candidates that using our IIBA IIBA-CCA Test Questions and test answers can easily verify their quality. GetValidTest IIBA IIBA-CCA certification training ensured their success.

IIBA Certificate in Cybersecurity Analysis Sample Questions (Q64-Q69):

NEW QUESTION # 64
What does non-repudiation mean in the context of web security?

- A. Providing permission to use web server resources according to security policies and specified procedures, so that the activity can be audited
- B. Ensuring that all traffic between web servers must be securely encrypted
- C. Providing the sender of a message with proof of delivery, and the receiver with proof of the sender's identity
- D. Ensuring that all data has not been altered in an unauthorized manner while being transmitted between web servers

Answer: C

Explanation:
Non-repudiation is a security property that provides verifiable evidence of an action or communication so that the parties involved cannot credibly deny their participation later. In web security, it most commonly means being able to prove who sent a message or performed a transaction and, in many cases, that the message was received and recorded. This is why option D is correct: it captures the idea of giving the receiver proof of the sender's identity and giving the sender evidence that the message or transaction was delivered or accepted.
Cybersecurity guidance typically associates non-repudiation with digital signatures, strong identity binding, and protected audit evidence. A digital signature uses asymmetric cryptography so that only the holder of a private key can sign, while anyone with the public key can verify the signature. When combined with trusted certificates, accurate time sources, and protected logs, this creates strong accountability. Non-repudiation also depends on maintaining the integrity of supporting evidence, such as tamper-resistant audit logs, secure log retention, and controlled access to signing keys.
It is different from confidentiality (encryption of traffic), and different from integrity alone (preventing unauthorized modification). It is also different from authorization and auditing, which support accountability but do not, by themselves, provide cryptographic-grade proof that a specific entity performed a specific action. Non-repudiation is especially important for high-trust transactions such as approvals, payments, and legally binding communications.

NEW QUESTION # 65
Which scenario is an example of the principle of least privilege being followed?

- A. All application and database administrators have full permissions to every application in the company
- B. Certain users are granted administrative access to their network account, in case they need to install a web-app
- C. An application administrator has full permissions to only the applications they support
- D. A manager who is conducting performance appraisals is granted access to HR files for all employees

Answer: C

Explanation:
The principle of least privilege requires that users, administrators, services, and applications are granted only the minimum access necessary to perform authorized job functions, and nothing more. Option A follows this principle because the administrator's elevated permissions are limited in scope to the specific applications they are responsible for supporting. This reduces the attack surface and limits blast radius: if that administrator account is compromised, the attacker's reach is constrained to only those applications rather than the entire enterprise environment.
Least privilege is typically implemented through role-based access control, separation of duties, and privileged access management practices. These controls ensure privileges are assigned based on defined roles, reviewed regularly, and removed when no longer required. They also promote using standard user accounts for routine tasks and reserving administrative actions for controlled, auditable sessions. In addition, least privilege supports stronger accountability through logging and change tracking, because fewer people have the ability to make high-impact changes across systems.
The other scenarios violate least privilege. Option B grants excessive enterprise-wide permissions, creating unnecessary risk and enabling widespread damage from mistakes or compromise. Option C provides "just in case" administrative access, which cybersecurity guidance explicitly discourages because it increases exposure without a validated business need. Option D is overly broad because access to all HR files exceeds what is required for performance appraisals, which typically should be limited to relevant employee records only.

NEW QUESTION # 66
What is the definition of privileged account management?

- A. Applying identity and access management controls
- B. Managing senior leadership and executive accounts
- C. Managing independent authentication of accounts
- D. Establishing and maintaining access rights and controls for users who require elevated privileges to an entity for an administrative or support function

Answer: D

Explanation:
Privileged account management refers to the governance and operational controls used to administer accounts that have elevated permissions beyond standard user access. Privileged accounts can change system configurations, create or modify users, access sensitive datasets, disable security tools, and administer core infrastructure such as servers, databases, directories, network devices, and cloud consoles. Because misuse of privileged access can quickly lead to large-scale compromise, cybersecurity frameworks treat privileged access as a high-risk area requiring stronger safeguards than normal accounts.
The definition in option A is correct because it captures the core purpose of privileged account management: establishing and maintaining access rights and controls specifically for roles that must perform administrative or support functions. In practice, this includes ensuring privileges are granted only when justified, scoped to the minimum necessary, and reviewed regularly. It also includes controls such as separation of duties, approval workflows, time-bound elevation, credential vaulting, rotation of privileged passwords and keys, multifactor authentication, and detailed logging of privileged sessions for monitoring and audit.
Option B is too broad because privileged account management is a specialized subset of identity and access management focused on elevated access. Option C is incorrect because privilege is defined by permissions, not job title. Option D describes an authentication concept, not the full management lifecycle of privileged access.

NEW QUESTION # 67
Which of the following would qualify as a multi-factor authentication pair?

- A. Password and Token
- B. Thumbprint and Encryption
- C. Encryption and Password
- D. Something You Know and Something You Are

Answer: D

Explanation:
Multi-factor authentication requires a user to prove identity using two or more different factor types. Cybersecurity standards describe the main factor categories as something you know (for example, a password or PIN), something you have (for example, a hardware token, smart card, or authenticator app producing a one-time code), and something you are (biometrics such as fingerprint, face, or iris). A valid MFA pair must come from different categories, not just two items from the same category or a mix of authentication with non-authentication concepts.
Option B is correct because it explicitly combines two distinct factor types: a knowledge factor and an inherence factor. This pairing is widely recognized as MFA because compromising one factor does not automatically compromise the other: an attacker who steals a password still needs the biometric, and spoofing a biometric does not provide the secret knowledge factor.
Option A is incorrect because "encryption" is not an authentication factor; it is a protection mechanism for confidentiality and integrity of data. Option D has the same problem: encryption is not a user factor. Option C can represent MFA in many real implementations if "token" is truly a possession factor; however, training materials and exam items often prefer the clearest, unambiguous factor-language pairing, which is why "Something You Know and Something You Are" is the best single answer here.

NEW QUESTION # 68
What common mitigation tool is used for directly handling or treating cyber risks?

- A. Standards
- B. Control
- C. Exit Strategy
- D. Business Continuity Plan

Answer: B

Explanation:
In cybersecurity risk management, risk treatment is the set of actions used to reduce risk to an acceptable level. The most common

tool used to directly treat or mitigate cyber risk is a control because controls are the specific safeguards that prevent, detect, or correct adverse events. Cybersecurity frameworks describe controls as measures implemented to reduce either the likelihood of a threat event occurring or the impact if it does occur. Controls can be technical (such as multifactor authentication, encryption, endpoint protection, network segmentation, logging and monitoring), administrative (policies, standards, training, access approvals, change management), or physical (badges, locks, facility protections). Regardless of type, controls are the direct mechanism used to mitigate identified risks.
An exit strategy is typically a vendor or outsourcing risk management concept focused on how to transition away from a provider or system; it supports resilience but is not the primary tool for directly mitigating a specific cyber risk. Standards guide consistency by defining required practices and configurations, but the standard itself is not the mitigation-controls implemented to meet the standard are. A business continuity plan supports availability and recovery after disruption, which is important, but it primarily addresses continuity and recovery rather than directly reducing the underlying cybersecurity risk in normal operations. Therefore, the best answer is the one that represents the direct implementation of safeguards: controls.

NEW QUESTION # 69
.....