100% Pass IIBA - Accurate IIBA-CCA Latest Mock Test

IIBA - ECBA TEST EXAM 2024 WITH 100% CORRECT ANSWERS

Which of the following is NOT part of the Business Analysis Core Concept Model (BACCM™)?

a) Change

b) Need

c) Requirements

d) StakeholderAnswer ✔✔- c) Requirements

Explanation

2.0 Business Analysis Key Concepts, 2.1 The Business Analysis Core Concept Model™, pages# 12-14 The Business Analysis Core Concept Model has six (6) elements to it, they are: 1. Changes 2. Solutions 3. Contexts 4. Values 5. Stakeholders 6. Needs

Decision-making falls under which competency category?

a) Business Knowledge

b) Critical Thinking and Problem Solving

c) Communication Skills

d) Interaction SkillsAnswer ✔✔- b) Critical Thinking and Problem Solving

Explanation

9.0 Underlying Competencies, 9.1 Analytical Thinking and Problem Solving, page #188. Decision Making is a competency that falls under the heading of Analytical Thinking and Problem Solving, providing a decision where critical thinking and problem solving has been applied is a competency that business analysts should demonstrate.

Which of the following is not a task in the Elicitation and Collaboration Knowledge Area?

BONUS!!! Download part of Lead1Pass IIBA-CCA dumps for free: https://drive.google.com/open?id=1F2iXo5emndeG1PXhW8iUDekDNGjI8HMR

Lead1Pass gives you unlimited online access to IIBA-CCA certification practice tools. You can instantly download the IIBA-CCA test engine and install it on your PDF reader, laptop or phone, then you can study it in the comfort of your home or while at office. Our IIBA-CCA test engine allows you to study anytime and anywhere. In addition, you can set the time for each test practice of IIBA-CCA simulate test. The intelligence and customizable IIBA-CCA training material will help you get the IIBA-CCA certification successfully.

The optimization of IIBA-CCA training questions is very much in need of your opinion. If you find any problems during use, you can give us feedback. We will give you some benefits as a thank you. You will get a chance to update the system of IIBA-CCA Real Exam for free. Of course, we really hope that you can make some good suggestions after using our IIBA-CCA study materials. We hope to grow with you and help you get more success in your life.

>> IIBA-CCA Latest Mock Test <<

IIBA IIBA-CCA Dumps - Pass Exam And Build Successful Career

Our IIBA-CCA exam questions have been widely acclaimed among our customers, and the good reputation in industry prove that choosing our study materials would be the best way for you, and help you gain the IIBA-CCA certification successfully. With about ten years' research and development we still keep updating our IIBA-CCA Prep Guide, in order to grasp knowledge points in

accordance with the exam, thus your study process would targeted and efficient.

IIBA IIBA-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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.
Topic 4	• 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 5	• 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 Certificate in Cybersecurity Analysis Sample Questions (Q50-Q55):

NEW QUESTION # 50
Which organizational area would drive a cybersecurity infrastructure Business Case?

- A. Finance
- B. Legal
- C. IT
- D. Risk

Answer: D

Explanation:
A cybersecurity infrastructure business case is typically driven by the Risk function because the justification for security investments is grounded in reducing enterprise risk to an acceptable level and aligning with the organization's risk appetite and regulatory obligations. Risk-focused teams (often working with the CISO and security governance) translate threats, vulnerabilities, and control gaps into business impact terms such as likelihood of adverse events, potential operational disruption, financial exposure, regulatory penalties, and reputational harm. This framing is what a formal business case requires: a clear problem statement, quantified or prioritized risk scenarios, expected risk reduction from proposed controls, and how residual risk compares to tolerance thresholds. While IT usually leads implementation and provides architecture, sizing, and operational cost estimates, IT alone does not typically "drive" the business case without the risk rationale that explains why the investment is necessary and what enterprise outcomes it protects. Legal contributes requirements related to compliance, contracts, and breach handling, but it generally supports rather than owns investment prioritization. Finance evaluates budgeting, funding options, and return-on-investment assumptions, yet it relies on risk inputs to understand why the spend is warranted and what loss exposure is being reduced.
Therefore, the organizational area most responsible for driving a cybersecurity infrastructure business case-by defining the risk problem, articulating risk-based benefits, and enabling executive decision-making-is Risk.
Bottom of Form

NEW QUESTION # 51
In the OSI model for network communication, the Session Layer is responsible for:

- A. establishing a connection and terminating it when it is no longer needed.

- B. adding appropriate network addresses to packets.
- C. transmitting the data on the medium.
- D. presenting data to the receiver in a form that it recognizes.

Answer: A

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 # 52
Which of the following activities are part of the business analyst's role in ensuring compliance with security policies?

- A. Ensuring that security policies are reflected in the solution requirements
- B. Auditing enterprise security policies to ensure that they comply with regulations
- C. Testing applications to identify potential security holes
- D. Checking to ensure that business users follow the security requirements

Answer: A

Explanation:
Business analysts support cybersecurity compliance primarily by ensuring that security and privacy expectations are translated into clear, testable requirements that are built into the solution. This includes eliciting applicable organizational security policies, standards, and control objectives, then mapping them into functional and non-functional requirements such as authentication methods, role-based access, logging and audit trail needs, encryption requirements, session controls, data retention, and segregation of duties.
When security policies are reflected in the solution requirements, they become part of the delivery lifecycle: they can be designed, implemented, validated in testing, and verified during acceptance. This creates traceability from policy to requirement to control implementation, which is essential for audits and for demonstrating due diligence.
Option A is typically the responsibility of governance, risk, and compliance functions or internal audit, not the BA. Option C is usually performed by security testing specialists, QA teams, or application security engineers using techniques like SAST, DAST, and penetration testing. Option D is largely an operational management and compliance enforcement function, supported by training, monitoring, and disciplinary processes. The BA's distinct contribution is ensuring policy-driven security controls are captured in requirements and embedded into the solution design and delivery artifacts.

NEW QUESTION # 53
Which of the following factors is most important in determining the classification of personal information?

- A. Accessibility
- B. Integrity
- C. Confidentiality
- D. Availability

Answer: C

Explanation:
Personal information is classified primarily based on the harm that could result from unauthorized disclosure, which maps directly to the confidentiality objective. Cybersecurity and privacy governance frameworks treat personal data as sensitive because exposure

can lead to identity theft, fraud, discrimination, personal safety risks, and loss of privacy. Organizations also face regulatory penalties, contractual consequences, and reputational damage when personal data is disclosed without authorization. For this reason, when determining classification, the first and most influential question is typically: "What is the impact if this data becomes known to someone who should not have it?" That impact assessment drives the required protection level and handling rules.
Confidentiality-focused controls then follow from the classification decision, including least privilege and role-based access, strong authentication, encryption at rest and in transit, secure key management, data loss prevention where appropriate, logging and monitoring of access to sensitive records, and strict sharing/transfer procedures.
Integrity and availability matter for personal information, but they are usually secondary in classification decisions. Integrity affects trustworthiness and correctness (for example, incorrect medical or payroll data), and availability affects the ability to access records when needed. However, the defining sensitivity of personal information is that it must not be disclosed improperly. "Accessibility" is not a core security objective used in standard classification models; it is an operational usability concept that is managed through access design after sensitivity is established.

NEW QUESTION # 54
Why is directory management important for cybersecurity?

- A. It allows all application security to be managed through a single interface
- B. It controls access to folders and files on the network
- C. It prevents outside agents from viewing confidential company information
- D. It prevents outsiders from knowing personal information about employees

Answer: B

Explanation:
Directory management is important because it provides a centralized way to define identities, groups, roles, and permissions, which directly determines who can access network resources. In most enterprises, directory services store user and service accounts and then integrate with file servers, applications, email platforms, VPN, and cloud services. This integration enables consistent enforcement of authorization rules such as group-based access to shared folders and files, role-based access control, and least privilege. Option D captures this core security purpose: directory management is a foundational control mechanism for governing access to networked resources.
From a cybersecurity controls perspective, directory management supports secure onboarding and offboarding, ensuring that new users receive only appropriate permissions and that departing users are disabled promptly to reduce insider and external risk. It also strengthens authentication by enabling enterprise-wide policies such as password rules, account lockouts, multi-factor authentication integration, and conditional access. In addition, centralized directories improve auditability: administrators can review memberships and entitlements, monitor privileged group changes, and generate logs that support investigations and compliance reporting.
The other options are either too broad or not primarily about directory management. While directories help protect confidential information indirectly, their direct function is not "preventing outside agents" by itself; it is enforcing access rules. They also do not manage all application security through one interface, and preventing outsiders from knowing employee personal information is a privacy objective, not the main purpose of directory management.
Top of Form

NEW QUESTION # 55
.....

- Easily Accessible IIBA IIBA-CCA PDF □ Download " IIBA-CCA " for free by simply searching on " www.prep4sures.top " □IIBA-CCA Test Collection
- 2026 IIBA IIBA-CCA: Certificate in Cybersecurity Analysis Latest Mock Test □ Search for ➠ IIBA-CCA □ on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □IIBA-CCA Valid Test Cram
- IIBA-CCA Latest Mock Test | Amazing Pass Rate For IIBA-CCA: Certificate in Cybersecurity Analysis | Exam IIBA-CCA Objectives □ The page for free download of " IIBA-CCA " on □ www.vce4dumps.com □ will open immediately □ □IIBA-CCA Valid Exam Sims
- 2026 IIBA IIBA-CCA: Certificate in Cybersecurity Analysis Latest Mock Test □ The page for free download of ⇛ IIBA-CCA ⇚ on 《 www.pdfvce.com 》 will open immediately □IIBA-CCA Test Collection
- 100% Pass Quiz 2026 IIBA-CCA: Marvelous Certificate in Cybersecurity Analysis Latest Mock Test □ Copy URL [www.vceengine.com] open and search for ✔ IIBA-CCA □✔□ to download for free □IIBA-CCA New Soft Simulations
- Valid IIBA IIBA-CCA Latest Mock Test - IIBA-CCA Free Download □ Easily obtain free download of ➠ IIBA-CCA □ by searching on ➤ www.pdfvce.com □ □IIBA-CCA New Soft Simulations
- Valid IIBA IIBA-CCA Latest Mock Test - IIBA-CCA Free Download □ Easily obtain free download of { IIBA-CCA } by searching on ✔ www.prep4away.com □✔□ □New IIBA-CCA Exam Duration
- courses.dbstudios.co.ke, qiita.com, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.alreemsedu.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, 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.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New IIBA-CCA dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=1F2iXo5emndeG1PXhW8iUDekDNGjI8HMR