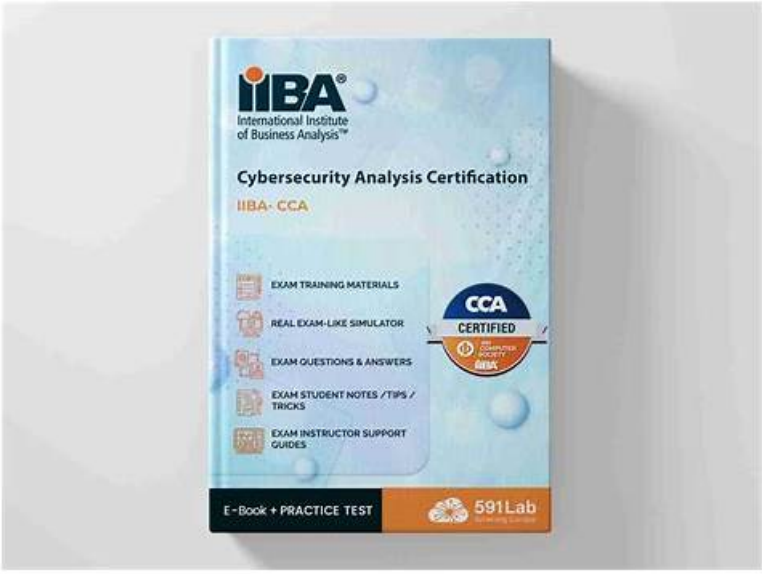
100% Pass IIBA-CCA - Certificate in Cybersecurity Analysis Pass-Sure Exam Sims



BTW, DOWNLOAD part of Getcertkey IIBA-CCA dumps from Cloud Storage: https://drive.google.com/open?id=1QyCcHIFLiOb8wfjyiHKII3r4d7Nh_mzc

At the moment you come into contact with our IIBA-CCA learning guide you can enjoy our excellent service. You can ask our staff about what you want to know. After full understanding, you can choose to buy our IIBA-CCA exam questions. If you use the IIBA-CCA study materials, you have problems that you cannot solve. Just contact with us via email or online, we will deal with you right away. And we offer 24/7 online service. So if you have any problem, you can always contact with us no matter any time it is.

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	• 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 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 Exam Sims <<

Authorized IIBA-CCA Exam Sims & Guaranteed IIBA IIBA-CCA Exam Success with The Best IIBA-CCA Testking Exam Questions

IIBA-CCA study guide provides free trial services, so that you can gain some information about our study contents, topics and how to make full use of the software before purchasing. It's a good way for you to choose what kind of IIBA-CCA training prep is suitable and make the right choice to avoid unnecessary waste. Our purchase process is of the safety and stability if you have any trouble in the purchasing IIBA-CCA practice materials or trail process, you can contact us immediately.

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

NEW QUESTION # 49
What is the "impact" in the context of cybersecurity risk?

- A. The probability that a breach will occur within a given period of time
- B. The magnitude of harm that can be expected from unauthorized information use
- C. The potential for violation of privacy laws and regulations from a cybersecurity breach
- D. The financial costs to the organization resulting from a breach

Answer: B

Explanation:
In cybersecurity risk management, impact refers to the severity of adverse consequences if a threat event occurs and successfully affects information or systems. It is the "so what" of a risk scenario: how much damage the organization, its customers, or other stakeholders could experience when confidentiality, integrity, or availability is compromised. Impact commonly includes multiple dimensions such as operational disruption, loss of critical services, harm to customers, legal or regulatory exposure, reputational damage, and direct and indirect financial loss. Because these consequences can extend beyond money, impact is broader than just costs and also includes mission failure, safety implications, loss of competitive advantage, and degradation of trust.
Option D captures this correctly by describing impact as the magnitude of harm expected from unauthorized use of information. Option C describes likelihood, not impact, because it focuses on probability over time. Option B is only one component of impact, since financial cost is important but does not fully represent business, legal, and operational consequences. Option A is also a possible consequence but is narrower than the full impact concept. Cybersecurity risk scoring typically combines likelihood and impact to prioritize treatment, ensuring high-impact scenarios receive attention even when probabilities vary.

NEW QUESTION # 50
The process by which organizations assess the data they hold and the level of protection it should be given based on its risk to loss or harm from disclosure, is known as:

- A. information categorization.
- B. information classification.
- C. internal audit.
- D. vulnerability assessment.

Answer: B

Explanation:
Information classification is the formal process of evaluating the data an organization creates or holds and assigning it a sensitivity level so the organization can apply the right safeguards. Cybersecurity policies describe classification as the foundation for consistent protection because it links the potential harm from unauthorized disclosure, alteration, or loss to specific handling and control requirements. Typical classification labels include Public, Internal, Confidential, and Restricted, though names vary by organization. Once data is classified, required protections can be specified, such as encryption at rest and in transit, access restrictions based on least privilege, approved storage locations, monitoring requirements, retention periods, and secure disposal methods.
This is not a vulnerability assessment, which focuses on identifying weaknesses in systems, applications, or configurations. It is also not an internal audit, which evaluates whether controls and processes are being followed and are effective. Option D, information categorization, is often used in some frameworks to describe assigning impact levels (for example, confidentiality, integrity, availability impact) to information types or systems, mainly to drive control baselines. While related, the question specifically emphasizes assessing data and deciding the level of protection based on risk from disclosure, which aligns most directly with classification programs used to govern labeling and handling rules across the organization.
A strong classification program improves security consistency, supports compliance, reduces accidental exposure, and helps prioritize controls for the most sensitive information assets.

NEW QUESTION # 51

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

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

Answer: D

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
What privacy legislation governs the use of healthcare data in the United States?

- A. PIPEDA
- B. PCI-DSS
- C. HIPAA
- D. Privacy Act

Answer: C

Explanation:
In the United States, HIPAA, the Health Insurance Portability and Accountability Act, is the primary federal framework that governs how certain healthcare information must be protected and used. In cybersecurity and compliance documentation, HIPAA is most often discussed through its implementing rules, especially the Privacy Rule and the Security Rule. The Privacy Rule establishes when protected health information may be used or disclosed and grants individuals rights over their health information. The Security Rule focuses specifically on safeguarding electronic protected health information by requiring administrative, physical, and technical safeguards.
From a security controls perspective, HIPAA-driven programs typically include risk analysis and risk management, policies and workforce training, access controls based on least privilege, unique user identification, authentication controls, audit logging, integrity protections, transmission security such as encryption for data in transit, and contingency planning such as backups and disaster recovery. HIPAA also expects organizations to manage third-party risk through appropriate agreements and oversight when vendors handle protected health information.
The other options do not fit the question. The Privacy Act generally applies to U.S. federal agencies' handling of personal records, PIPEDA is a Canadian privacy law, and PCI-DSS is an industry security standard focused on payment card data rather than healthcare data. Therefore, HIPAA is the correct legislation for U.S. healthcare data protection requirements.

NEW QUESTION # 53
Violations of the EU's General Data Protection Regulations GDPR can result in:

- A. mandatory upgrades of the security infrastructure.
- B. fines of €20 million or 4% of annual turnover, whichever is less.
- C. a complete audit of the enterprise's security processes.
- 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 # 54
.....

BTW, DOWNLOAD part of Getcertkey IIBA-CCA dumps from Cloud Storage: https://drive.google.com/open?id=1QyCcHIFLiOb8wfjyiHKII3r4d7Nh_mzc