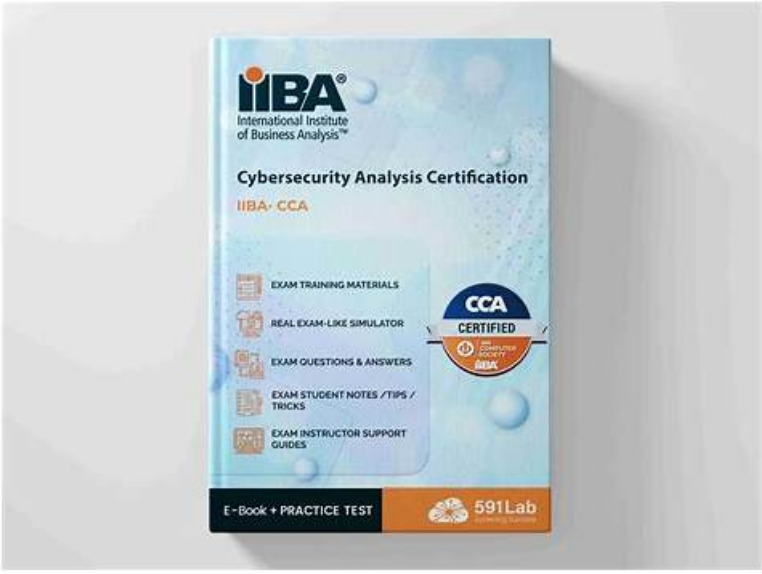
IIBA-CCA Examcollection & Practice IIBA-CCA Test Online



P.S. Free & New IIBA-CCA dumps are available on Google Drive shared by Prep4cram: https://drive.google.com/open?id=14oBa8EG5kkEdb372RPFGr4H6VgMG90ME

A good brand is not a cheap product, but a brand that goes well beyond its users' expectations. The value of a brand is that the IIBA-CCA exam questions are more than just exam preparation tool -- it should be part of our lives, into our daily lives. Do this, therefore, our IIBA-CCA question guide has become the industry well-known brands, but even so, we have never stopped the pace of progress, we have been constantly updated the IIBA-CCA real study guide. Our IIBA-CCA real study guide provides users with comprehensive learning materials, so that users can keep abreast of the progress of The Times.

Our company is a professional certificate test materials provider, and we are in the leading position in providing valid and effective exam materials. IIBA-CCA exam braindumps are high quality, and it also contain certain questions and answers, and it will be enough for you to pass the exam. Besides, in order to let you have a deeper understanding of what you are going to buy, we offer you free demo to have a try before buying IIBA-CCA Training Materials. We offer you free update for 365 days after purchasing, and the update version will be sent to your email address automatically.

>> IIBA-CCA Examcollection <<

Practice IIBA-CCA Test Online - IIBA-CCA Practice Test Online

IIBA IIBA-CCA is one of the important certification exams. Prep4cram's experienced IT experts through their extensive experience and professional IT expertise have come up with IT certification exam study materials to help people pass IIBA Certification IIBA-CCA Exam successfully. Prep4cram's providing learning materials can not only help you 100% pass the exam, but also provide you a free one-year update service.

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 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	• 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 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 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 (Q65-Q70):

NEW QUESTION # 65
The opportunity cost of increased cybersecurity is that:

- A. identifying and securing assets and systems requires resources that are therefore not available to other initiatives.
- B. costs of meeting regulations are constantly increasing.
- C. the potential cost of implementing security will always be less than the potential risk from a breach of customer data.
- D. cybersecurity adds considerably to the cost of developing new business systems.

Answer: A

Explanation:
Opportunity cost is a core enterprise-risk and economics concept: when an organization allocates limited resources to one activity, it reduces what is available for other priorities. Increasing cybersecurity typically requires money, skilled personnel time, executive attention, tooling, and operational capacity. Those resources could otherwise be used for revenue-generating work such as new product features, customer experience improvements, system modernization, market expansion, or process automation. That tradeoff is exactly what option D describes, making it the correct answer.
Cybersecurity documents stress that risk treatment decisions must balance risk reduction against cost, feasibility, and business impact. While stronger security can reduce the likelihood and impact of incidents, it can also introduce friction (extra approval steps, stronger authentication, segmentation), slow delivery when changes require additional reviews, and demand ongoing operational effort (monitoring, patching, vulnerability remediation, access recertification, incident response testing). These impacts are not arguments against security; they are the reason governance processes prioritize controls based on the most critical assets, highest-risk threats, and compliance requirements.
Option A may be true in some cases, but it describes a direct cost, not the broader economic concept of opportunity cost. Option B is a trend statement and not the definition. Option C is incorrect because security spend is not always less than breach risk; organizations must evaluate cost-benefit and acceptable residual risk rather than assume a universal rule.

NEW QUESTION # 66
How should categorization information be used in business impact analysis?

- A. To determine the time and effort required for business impact assessment
- B. To identify discrepancies between the security categorization and the expected business impact
- C. To ensure that systems are designed to support the appropriate security categorization
- D. To assess whether information should be shared with other systems

Answer: B

NEW QUESTION # 67
How is a risk score calculated?

- A. Based on past experience regarding the risk
- B. Based on an assessment of threats by the cyber security team
- C. Based on the confidentiality, integrity, and availability characteristics of the system

- D. Based on the combination of probability and impact

Answer: D

Explanation:
A risk score is commonly calculated by combining two core factors: how likely a risk scenario is to occur and how severe the consequences would be if it did occur. This is often described in cybersecurity risk documentation as likelihood times impact, or as a structured mapping using a risk matrix. Probability or likelihood reflects the chance that a threat event will exploit a vulnerability under current conditions. It may consider elements such as threat activity, exposure, ease of exploitation, control strength, and historical incident patterns. Impact reflects the magnitude of harm to the organization, usually measured across business disruption, financial loss, legal or regulatory exposure, reputational damage, and harm to confidentiality, integrity, or availability.
While confidentiality, integrity, and availability are essential for understanding what matters and can influence impact ratings, they are typically inputs into impact determination rather than the full scoring method by themselves. Past experience and expert threat assessment can inform likelihood estimates, but they are not the standard calculation model on their own. The key concept is that risk must reflect both chance and consequence; a highly impactful event with very low likelihood may be scored similarly to a moderate impact event with high likelihood depending on the organization's methodology.
Therefore, the most accurate description of how a risk score is calculated is the combination of probability and impact, enabling prioritization and consistent risk treatment decisions.

NEW QUESTION # 68
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. internal audit.
- B. information categorization.
- C. information classification.
- D. vulnerability assessment.

Answer: C

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 # 69
What is the purpose of Digital Rights Management DRM?

- A. To control the use, modification, and distribution of copyrighted works
- B. To ensure that intellectual property remains under the full control of the originating enterprise
- C. To ensure that all attempts to access information are tracked, logged, and auditable
- D. To ensure that corporate files and data cannot be accessed by unauthorized personnel

Answer: A

Explanation:
Digital Rights Management is a set of technical mechanisms used to enforce the permitted uses of digital content after it has been delivered to a user or device. Its primary purpose is to control how copyrighted works are accessed and used, including restricting

copying, printing, screen capture, forwarding, offline use, device limits, and redistribution. DRM systems commonly apply encryption to content and then rely on a licensing and policy enforcement component that checks whether a user or device has the right to open the content and under what conditions. These conditions can include time-based access (expiry), geographic limitations, subscription status, concurrent use limits, or restrictions on modification and export.
This aligns precisely with option B because DRM is fundamentally about usage control of copyrighted digital works, such as music, movies, e-books, software, and protected media streams. In cybersecurity documentation, DRM is often discussed alongside content protection, anti-piracy measures, and license compliance. It differs from general access control and audit logging: access control determines who may enter a system or open a resource, while auditing records actions for accountability. DRM extends beyond simple access by enforcing what a legitimate user can do with the content once accessed.
Option A describes audit logging, option C describes general authorization and data access control, and option D is closer to broad information rights management goals but is less precise than the standard definition focused on controlling use and distribution of copyrighted works.

NEW QUESTION # 70
.....

The clients can consult our online customer service before and after they buy our IIBA-CCA study materials. We provide considerate customer service to the clients. Before the clients buy our IIBA-CCA study materials they can consult our online customer service personnel about the products' version and price and then decide whether to buy them or not. After the clients buy the IIBA-CCA study materials they can consult our online customer service about how to use them and the problems which occur during the process of using. If the clients fail in the test and require the refund our online customer service will reply their requests quickly and deal with the refund procedures promptly. In short, our online customer service will reply all of the clients' questions about the IIBA-CCA Study Materials timely and efficiently.