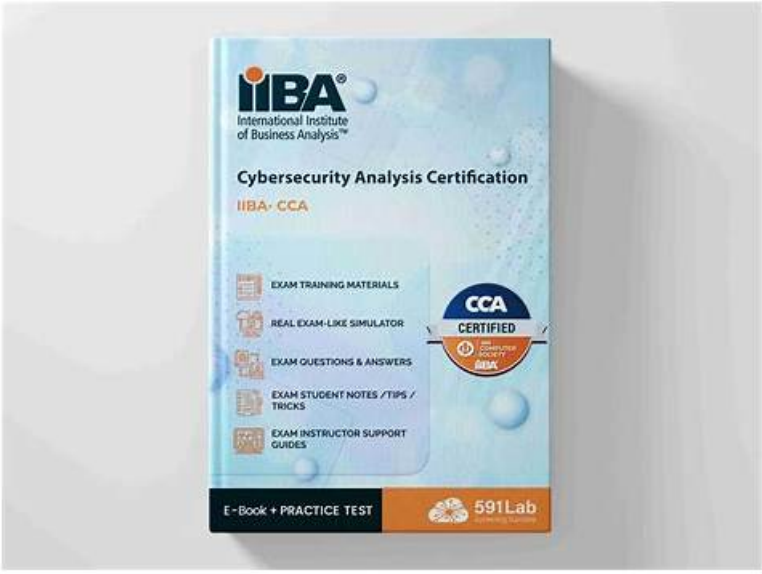
IIBA IIBA-CCA자격증덤프, IIBA-CCA시험대비공부문제



PassTIP는IT업계전문가들이 그들의 노하우와 몇 년간의 경험 등으로 자료의 정확도를 높여 응시자들의 요구를 만족시켜 드립니다. 우리는 꼭 한번에IIBA IIBA-CCA시험을 패스할 수 있도록 도와드릴 것입니다. 여러분은IIBA IIBA-CCA시험자료 구매로 제일 정확하고 또 최신시험버전의 문제와 답을 사용할 수 있습니다. Pass4Tes의 인증시험적중 율은 아주 높습니다. 때문에 많은 IT인증시험준비중인분들에세 많은 편리를 드릴수 있습니다.100%정확도 100%신뢰.여러분은 마음편히 응시하시면 됩니다.

IIBA IIBA-CCA 시험요강:

주제	소개
주제 1	• 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.
주제 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.
주제 3	• 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.
주제 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.

>> IIBA IIBA-CCA자격증덤프 <<

IIBA-CCA시험대비 공부문제, IIBA-CCA합격보장 가능 시험대비자료

덤프는 구체적인 업데이트주기가 존재하지 않습니다. 하지만 저희는 수시로 IIBA IIBA-CCA 시험문제 변경을 체크하여IIBA IIBA-CCA덤프를 가장 최신버전으로 업데이트하도록 최선을 다하고 있습니다. IIBA IIBA-CCA덤프를 구매하면 1년간 업데이트될떼마다 최신버전을 구매시 사용한 메일로 전송해드립니다.

최신 Cybersecurity Analysis IIBA-CCA 무료샘플문제 (Q62-Q67):

질문 # 62
Which of the following factors is most important in determining the classification of personal information?

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

정답：C

설명：
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.

질문 # 63
What business analysis deliverable would be an essential input when designing an audit log report?

- A. Internal Audit Report
- B. Risk Log
- C. Future State Business Process
- D. Access Control Requirements

정답：D

설명：
Designing an audit log report requires clarity on who is allowed to do what, which actions are considered security-relevant, and what evidence must be captured to demonstrate accountability. Access Control Requirements are the essential business analysis deliverable because they define roles, permissions, segregation of duties, privileged functions, approval workflows, and the conditions under which access is granted or denied. From these requirements, the logging design can specify exactly which events must be recorded, such as authentication attempts, authorization decisions, privilege elevation, administrative changes, access to sensitive records, data exports, configuration changes, and failed access attempts. They also help determine how logs should attribute actions to unique identities, including service accounts and delegated administration, which is critical for auditability and non-repudiation.
Access control requirements also drive necessary log fields and report structure: user or role, timestamp, source, target object, action, outcome, and reason codes for denials or policy exceptions. Without these requirements, an audit log report can become either too sparse to support investigations and compliance, or too noisy to be operationally useful.
A risk log can influence priorities, but it does not define the authoritative set of access events and entitlements that must be auditable. A future state process can provide context, yet it is not as precise as access rules for determining what to log. An internal audit report may highlight gaps, but it is not the primary design input compared to formal access control requirements.

질문 # 64
What stage of incident management would "strengthen the security from lessons learned" fall into?

- A. Recovery
- B. Remediation

- C. Response
- D. Detection

정답：B

설명：
"Strengthen the security from lessons learned" fits the remediation stage because it focuses on eliminating root causes and improving controls so the same incident is less likely to recur. In incident management lifecycles, response is about immediate actions to contain and manage the incident (triage, containment, eradication actions in progress, communications, and preserving evidence). Detection is the identification and confirmation stage (alerts, analysis, validation, and initial classification). Recovery is restoring services to normal operation and verifying stability, including bringing systems back online, validating data integrity, and meeting recovery objectives.
After the environment is stable, organizations conduct a post-incident review and then implement corrective and preventive actions. That work is remediation: closing exploited vulnerabilities, hardening configurations, rotating credentials and keys, tightening access and privileged account controls, improving monitoring and logging coverage, updating firewall rules or segmentation, refining secure development practices, and correcting process gaps such as weak change management or incomplete asset inventory. Remediation also includes updating policies and playbooks, enhancing detection rules based on observed attacker techniques, and training targeted groups if human factors contributed.
Cybersecurity guidance emphasizes documenting lessons learned, assigning owners and deadlines, validating fixes, and tracking completion because "lessons learned" without implemented change does not reduce risk. The defining characteristic is durable improvement to the control environment, which is why this activity belongs to remediation rather than response, detection, or recovery.

질문 # 65
What does non-repudiation mean in the context of web security?

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

정답：D

설명：
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.

질문 # 66
Which organizational area would drive a cybersecurity infrastructure Business Case?

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

정답：D

질문 # 67
.....

IIBA인증 IIBA-CCA시험은 중요한 IT인증자격증을 취득하는 필수시험과목입니다IIBA인증 IIBA-CCA시험을 통과해야만 자격증 취득이 가능합니다.자격증을 많이 취득하면 자신의 경쟁율을 높여 다른능력자에 의해 대체되는 일은 면할수 있습니다.PassTIP에서는IIBA 인증IIBA-CCA시험대비덤프를 출시하여 여러분이 IT업계에서 더 높은 자리에 오르도록 도움드립니다. 편한 덤프공부로 멋진 IT전문가의 꿈을 이루세요.

IIBA-CCA시험대비 공부문제: https://www.passtip.net/IIBA-CCA-pass-exam.html

- IIBA-CCA PDF ➡ IIBA-CCA시험내용 □ IIBA-CCA최고품질 덤프문제모음집 □ 지금➥ kr.fast2test.com □에서《 IIBA-CCA 》를 검색하고 무료로 다운로드하세요IIBA-CCA시험대비 최신 덤프자료
- IIBA-CCA인증시험공부 □ IIBA-CCA시험대비 덤프샘플 다운 □ IIBA-CCA시험대비 덤프샘플 다운 □ 《 IIBA-CCA 》를 무료로 다운로드하려면[www.itdumpskr.com]웹사이트를 입력하세요IIBA-CCA합격보장 가능 공부자료
- IIBA-CCA최신 시험기출문제 □ IIBA-CCA인증시험공부 □ IIBA-CCA최신 업데이트 덤프문제 □ 무료 다운로드를 위해➥ IIBA-CCA □를 검색하려면☀ www.koreadumps.com □☀□을(를) 입력하십시오IIBA-CCA시험대비 덤프샘플 다운
- IIBA-CCA자격증덤프 100% 유효한 시험공부자료 ☣ ▹ www.itdumpskr.com ◃의 무료 다운로드▹ IIBA-CCA ◃페이지가 지금 열립니다IIBA-CCA시험대비 최신 덤프자료
- IIBA-CCA합격보장 가능 공부자료 □ IIBA-CCA시험덤프공부 □ IIBA-CCA인증덤프 샘플체험 □ 지금➠ kr.fast2test.com □을(를) 열고 무료 다운로드를 위해《 IIBA-CCA 》를 검색하십시오IIBA-CCA시험덤프공부
- IIBA-CCA시험대비 최신 덤프자료 □ IIBA-CCA최신 업데이트 시험덤프문제 □ IIBA-CCA적중율 높은 시험덤프공부 □ 무료로 쉽게 다운로드하려면[www.itdumpskr.com]에서✔ IIBA-CCA □✔□를 검색하세요 IIBA-CCA시험대비 덤프샘플 다운
- IIBA-CCA자격증덤프 인증시험 덤프자료 □ 검색만 하면⇛ www.koreadumps.com ⇚에서□ IIBA-CCA □무료 다운로드IIBA-CCA인증시험공부
- 100% 합격보장 가능한 IIBA-CCA자격증덤프 인증공부자료 □ ➽ www.itdumpskr.com □에서（ IIBA-CCA ）를 검색하고 무료로 다운로드하세요IIBA-CCA인기자격증 시험덤프 최신자료
- IIBA-CCA자격증덤프 인기시험 기출문제 □ ➤ www.koreadumps.com □을(를) 열고□ IIBA-CCA □를 검색하여 시험 자료를 무료로 다운로드하십시오IIBA-CCA인증시험대비 공부자료
- IIBA-CCA인증시험대비 공부자료 □ IIBA-CCA시험대비 최신 덤프자료 □ IIBA-CCA인증시험공부 □ 검색만 하면《 www.itdumpskr.com 》에서➠ IIBA-CCA □무료 다운로드IIBA-CCA인증시험공부
- IIBA-CCA완벽한 시험기출자료 □ IIBA-CCA시험덤프공부 □ IIBA-CCA덤프문제모음 □ □ kr.fast2test.com □에서▶ IIBA-CCA ◀를 검색하고 무료 다운로드 받기IIBA-CCA시험덤프공부
- theoneox127018.blogozz.com, nicolesimb569942.dekaronwiki.com, sabrinayokz358053.theobloggers.com, pageoftoday.com, keiranrhok146297.blog-eye.com, kobimyyc809947.nizarblog.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, lillippmn851626.wannawiki.com, leakqwg630643.westexwiki.com, Disposable vapes