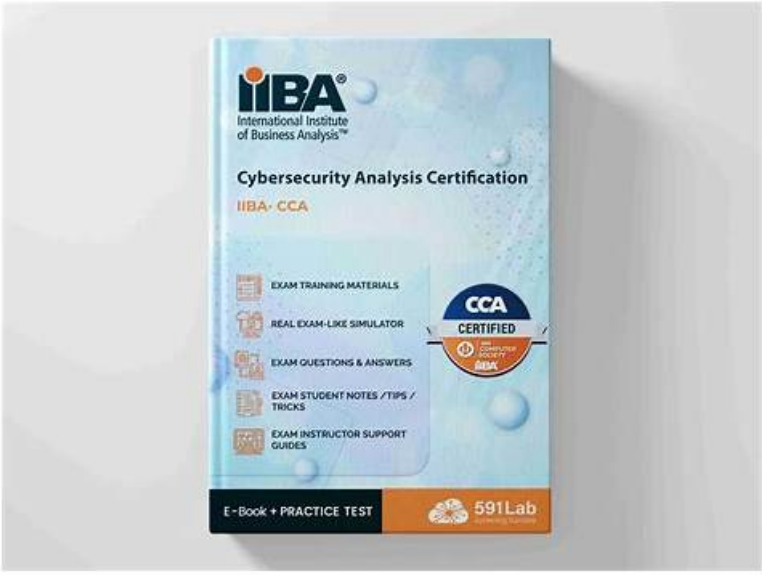
IIBA-CCA인증덤프문제완벽한시험기출문제



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.

IIBA IIBA-CCA 덤프의 PDF 버전과 Software 버전의 내용은 동일합니다. PDF버전은 프린트 가능한 버전으로서 단독구매하셔도 됩니다. Software 버전은 테스트용으로 PDF 버전 공부를 마친후 시험전에 실력테스트 가능합니다. Software 버전은 PDF버전의 보조용이기에 단독 판매하지 않습니다. 소프트웨어버전까지 필요하신 분은 PDF버전을 구입하실때 공동구매하셔야 합니다.

>> IIBA-CCA인증덤프문제 <<

IIBA-CCA인증덤프문제 최신 인기시험 기출문제모음

IIBA IIBA-CCA시험이 정말 어렵다는 말을 많이 들으신 만큼 저희 DumpTOP는IIBA IIBA-CCA덤프만 있으면IIBA IIBA-CCA시험이 정말 쉬워진다고 전해드리고 싶습니다. IIBA IIBA-CCA덤프로 시험패스하고 자격증 한방에 따보세요. 자격증 많이 취득하면 더욱 여유롭게 직장생활을 즐길수 있습니다.

IIBA IIBA-CCA 시험요강:

주제	소개
주제 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.
주제 2	• 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.
주제 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.
주제 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.

최신 Cybersecurity Analysis IIBA-CCA 무료샘플문제 (Q35-Q40):

질문 # 35
Where business process diagrams can be used to identify vulnerabilities within solution processes, what tool can be used to identify vulnerabilities within solution technology?

- A. Penetration Test
- B. Vulnerability-as-a-Service
- C. Security Patch
- D. Smoke Test

정답：A

설명：
Business process diagrams help analysts spot weaknesses in workflows, approvals, handoffs, and segregation of duties, but they do not directly test the technical security of the underlying applications, infrastructure, or configurations. To identify vulnerabilities within solution technology, cybersecurity practice uses penetration testing, which is a controlled, authorized simulation of real-world attacks against systems. A penetration test examines how a solution behaves under adversarial conditions and validates whether security controls actually prevent exploitation, not just whether they are designed on paper.
Penetration testing typically includes reconnaissance, enumeration, and attempts to exploit weaknesses in areas such as authentication, session management, access control, input handling, APIs, encryption usage, misconfigurations, and exposed services. Results provide evidence-based findings, including exploit paths, impact, affected components, and recommended remediations. This makes penetration testing especially valuable before go-live, after major changes, and periodically for high-risk systems to confirm the security posture remains acceptable.
The other options do not fit the objective. A security patch is a remediation action taken after vulnerabilities are known, not a method for discovering them. A smoke test is a basic functional check to confirm the system builds and runs; it is not a security assessment. Vulnerability-as-a-Service is a delivery model that may include scanning or testing, but the recognized tool or technique for identifying vulnerabilities in the technology itself in this context is a penetration test, which directly evaluates exploitability and real security impact.

질문 # 36
If a Business Analyst is asked to document the current state of the organization's web-based business environment, and recommend where cost savings could be realized, what risk factor must be included in the analysis?

- A. Impact Severity
- B. Organizational Risk Tolerance
- C. Application Vulnerabilities
- D. Threat Likelihood

정답：C

설명：
When analyzing a web-based business environment for potential cost savings, the Business Analyst must account for application vulnerabilities because they directly affect the organization's exposure to cyber attack and the true cost of operating a system. Vulnerabilities are weaknesses in application code, configuration, components, or dependencies that can be exploited to compromise confidentiality, integrity, or availability. In web environments, common examples include insecure authentication, injection flaws, broken access control, misconfigurations, outdated libraries, and weak session management.
Cost-saving recommendations frequently involve consolidating platforms, reducing tooling, lowering support effort, retiring controls, delaying upgrades, or moving to shared services. Without including known or likely vulnerabilities, the analysis can unintentionally recommend changes that reduce preventive and detective capability, increase attack surface, or extend the time vulnerabilities remain unpatched. Cybersecurity governance guidance emphasizes that technology rationalization must consider security posture: vulnerable applications often require additional controls (patching cadence, WAF rules, monitoring, code fixes, penetration testing, secure SDLC work) that carry ongoing cost. These costs are part of the system's "total cost of ownership" and should be weighed against proposed savings.
While impact severity and threat likelihood are important for overall risk scoring, the question asks what risk factor must be included when documenting the current state of a web-based environment. The most essential factor that ties directly to the environment's condition and drives remediation cost and exposure is application vulnerabilities.

질문 # 37
Separation of duties, as a security principle, is intended to:

- A. balance user workload.
- B. ensure that all security systems are integrated.
- C. optimize security application performance.
- D. prevent fraud and error.

정답：D

설명：
Separation of duties is a foundational access-control and governance principle designed to reduce the likelihood of misuse, fraud, and significant mistakes by ensuring that no single individual can complete a critical process end-to-end without independent oversight. Cybersecurity and audit frameworks describe this as splitting high-risk activities into distinct roles so that one person's actions are checked or complemented by another person's authority. This limits both intentional abuse, such as unauthorized payments or data manipulation, and unintentional errors, such as misconfigurations or accidental deletion of important records.
In practice, separation of duties is implemented by defining roles and permissions so that incompatible functions are not assigned to the same account. Common examples include separating the ability to create a vendor from the ability to approve payments, separating software development from production deployment, and separating system administration from security monitoring or audit log management. This is reinforced through role-based access control, approval workflows, privileged access management, and periodic access reviews that detect conflicting entitlements and privilege creep.
The value of separation of duties is risk reduction through accountability and control. When actions require multiple parties or independent review, it becomes harder for a single compromised account or malicious insider to cause large harm without detection. It also improves reliability by introducing checkpoints that catch mistakes earlier. Therefore, the correct purpose is to prevent fraud and error.

질문 # 38
A software product that supports threat detection, and compliance and security incident management, through the collection and analysis of security events and other data sources, is known as a:

- A. cloud access security broker (CASB).
- B. threat risk assessment (TRA).
- C. software as a service (SaaS).
- D. security information and event management system (SIEM).

정답：D

설명：
A security information and event management system (SIEM) is designed to centralize and analyze security-relevant data to support threat detection, compliance reporting, and incident management. SIEM platforms ingest logs and telemetry from many sources such as servers, endpoints, network devices, firewalls, intrusion detection systems, identity providers, cloud services, and business applications. They normalize and correlate these events so analysts can identify suspicious patterns that would be difficult to see in isolated logs, such as repeated failed logins followed by a successful login from an unusual location, privilege escalation, lateral movement indicators, or abnormal data access.
Cybersecurity operational guidance emphasizes SIEM value in three main areas. First, detection and alerting: correlation rules, behavioral analytics, and threat intelligence enrichment help surface high-risk activity. Second, incident response support: SIEM provides timelines, evidence preservation, triage context, and query capabilities that help responders scope and contain incidents. Third, compliance and audit readiness: centralized log retention, integrity controls, and reporting demonstrate that monitoring and control requirements are operating.
The other options do not match the definition. SaaS is a delivery model, not a specific security monitoring capability. A threat risk assessment is a process, not a software product for event collection and correlation. A CASB focuses on governing and protecting cloud application usage, whereas SIEM focuses on cross-environment event aggregation, correlation, and security operations monitoring.

질문 # 39
Which statement is true about a data warehouse?

- A. Data cleaning must be done on operational systems before the data is transferred to a data warehouse
- B. Data stored in a data warehouse is used for analytical purposes, not operational tasks
- C. The data warehouse must use the same data structures as production systems
- D. Data warehouses should act as a central repository for the data generated by all operational systems

정답：B

설명：
A data warehouse is designed primarily to support analytics, reporting, and decision-making rather than day-to-day transaction processing. Operational systems are optimized for fast inserts/updates and real-time business operations such as order entry, billing, or customer service workflows. In contrast, a warehouse consolidates data-often from multiple sources-into structures optimized for querying, trending, and historical analysis. From a cybersecurity and governance perspective, this distinction matters because warehouses frequently contain large volumes of aggregated, historical, and sometimes sensitive information, which can increase impact if confidentiality is breached. As a result, controls like strong access governance, role-based access, least privilege, segregation of duties, encryption, and audit logging are emphasized for warehouses to reduce insider misuse and limit exposure. Option B is false because warehouses often use different structures (for example, dimensional models) than production systems, specifically to improve analytical performance and usability. Option C can be true in some architectures, but it is not universally required; organizations may operate multiple warehouses, data marts, or lakehouse patterns, and not all operational data is appropriate to centralize due to privacy, cost, and regulatory constraints. Option D is incorrect because cleansing is commonly performed in dedicated integration pipelines and staging layers rather than changing operational systems to "pre-clean" data. Therefore, A is the best verified statement.

질문 # 40
.....