# 試験の準備方法-便利なIIBA-CCA復習教材試験-高品質なIIBA-CCAトレーニング費用


一回だけでIIBAのIIBA-CCA試験に合格したい？ CertShikenは君の欲求を満たすために存在するのです。CertShikenは君にとってベストな選択になります。ここには、私たちは君の需要に応じます。CertShikenのIIBAのIIBA-CCA問題集を購入したら、私たちは君のために、一年間無料で更新サービスを提供することができます。もし不合格になったら、私たちは全額返金することを保証します。

IIBAのIIBA-CCA試験に参加するのは大ブレークになる一方が、IIBA-CCA試験情報は雑多などの問題が注目している。たくさんの品質高く問題集を取り除き、我々CertShikenのIIBA-CCA問題集を選らんでくださいませんか。我々のIIBA-CCA問題集はあなたに質高いかつ完備の情報を提供し、成功へ近道のショットカットになります。

**>> IIBA-CCA復習教材 <<**

## IIBA-CCA実用的｜素晴らしいIIBA-CCA復習教材試験｜試験の準備方法 Certificate in Cybersecurity Analysisトレーニング費用

最近のレポートによると、複数のスキル証明書を所有している人は、上司によって昇格されやすくなっています。日常から離れて理想的な生活を求めるには、職場で高い得点を獲得し、試合に勝つために余分なスキルを習得しなければなりません。 IIBA-CCA試験問題は、あなたの夢をかなえるのに役立ちます。さらに、IIBA-CCAガイドトレントに関する詳細情報を提供するWebサイトにアクセスできます。 IIBA-CCA試験問題を試してみてください。そうすれば、IIBA-CCA試験に合格できることがわかります。

## IIBA IIBA-CCA 認定試験の出題範囲:

| トピック | 出題範囲 |
|---|---|
| トピック 1 | • 要件分析と設計定義: この領域では、サイバーセキュリティ要件を詳細に分析、構造化、指定し、利害関係者と組織の期待に応えながらセキュリティニーズに対応するソリューション設計を定義します。 |
| トピック 2 | • 戦略分析: この領域では、組織のサイバーセキュリティ体制の現状を評価し、ギャップとリスクを特定し、セキュリティニーズとビジネス目標を一致させる将来の状態と変更戦略を定義します。 |
| トピック 3 | • 引き出しとコラボレーション: この領域では、サイバーセキュリティ関連の要件と情報を関係者から収集し、関係者全員の間で効果的なコミュニケーションとコラボレーションを促進するための手法に焦点を当てています。 |

## IIBA Certificate in Cybersecurity Analysis 認定 IIBA-CCA 試験問題 (Q55-Q60):

**質問 # 55**
An internet-based organization whose address is not known has attempted to acquire personal identification details such as usernames and passwords by creating a fake website. This is an example of?

- A. Ransomware
- B. Breach
- C. Phishing
- D. Threat

**正解：C**

解説：
Creating a fake website to trick individuals into entering usernames and passwords is a classic example of phishing. Phishing is a social engineering technique where an attacker impersonates a trusted entity to deceive a victim into disclosing sensitive information (credentials, personal data, payment details) or taking an action that benefits the attacker (downloading malware, approving an MFA prompt, wiring funds). A counterfeit login page is commonly used in credential-harvesting campaigns: the victim believes they are authenticating to a legitimate service, but the credentials are captured by the attacker and later used for account takeover. This is not necessarily a breach yet because the question describes an attempt to acquire credentials; a breach would be confirmed unauthorized access or disclosure. While phishing is a kind of threat, "threat" is too broad compared to the specific described behavior. It is also not ransomware, which focuses on encrypting or locking data and demanding payment. Cybersecurity documentation emphasizes layered defenses against phishing: user awareness training, email and web filtering, domain and certificate validation, anti-spoofing controls, strong authentication (especially MFA resistant to prompt fatigue), password managers that reduce credential entry on lookalike domains, and monitoring for suspicious logins. Because the attack relies on deception through a fake website to steal credentials, the best match is phishing.

**質問 # 56**
Compliance with regulations is generally demonstrated through:

- A. independent audits of systems and security procedures.
- B. penetration testing by ethical hackers.
- C. extensive QA testing prior to system implementation.
- D. review of security requirements by senior executives and/or the Board.

**正解：A**

解説：
Regulatory compliance is generally demonstrated through independent audits because regulators, customers, and partners typically require objective evidence that required controls exist and operate effectively. An independent audit is performed by a qualified party that is not responsible for running the controls being assessed, which strengthens credibility and reduces conflicts of interest. Cybersecurity and governance documents describe audits as a formal method to verify compliance against defined criteria such as laws, regulations, contractual obligations, or control frameworks. Auditors review policies and procedures, inspect system configurations, sample access and change records, evaluate logging and monitoring, test incident response evidence, and validate that controls are consistently performed over time. The outcome is usually a report, attestation, or findings with remediation plans-artifacts commonly used to prove compliance.
A Board or executive review supports governance and oversight, but it does not, by itself, provide independent verification that controls are functioning. QA testing focuses on product quality and functional correctness; it may include security testing but does not typically satisfy regulatory evidence requirements for ongoing operational controls. Penetration testing is valuable for identifying exploitable weaknesses, yet it is a point-in-time technical exercise and does not comprehensively demonstrate compliance with procedural, administrative, and operational requirements such as access governance, retention, training, vendor oversight, and continuous monitoring. Therefore, independent audits are the standard mechanism to demonstrate compliance in a defensible, repeatable way.

**質問 # 57**
What terms are often used to describe the relationship between a sub-directory and the directory in which it is cataloged?

- A. Primary and Secondary
- B. Parent and Child
- C. Multi-factor Tokens
- D. Embedded Layers

**正解：B**

解説：
Directories are commonly organized in a hierarchical structure, where each directory can contain sub-directories and files. In this hierarchy, the directory that contains another directory is referred to as the parent, and the contained sub-directory is referred to as the child. This parent-child relationship is foundational to how file systems and many directory services represent and manage objects, including how paths are constructed and how inheritance can apply.
From a cybersecurity perspective, understanding parent and child relationships matters because access control and administration often follow the hierarchy. For example, permissions applied at a parent folder may be inherited by child folders unless inheritance is explicitly broken or overridden. This can simplify administration by allowing consistent access patterns, but it also introduces risk: overly permissive settings at a parent level can unintentionally grant broad access to many child locations, increasing the chance of unauthorized data exposure. Security documents therefore emphasize careful design of directory structures, least privilege at higher levels of the hierarchy, and regular permission reviews to detect privilege creep and misconfigurations.
The other options do not describe this standard hierarchy terminology. "Primary and Secondary" is more commonly used for redundancy or replication roles, not directory relationships. "Multi-factor Tokens" relates to authentication factors. "Embedded Layers" is not a st

**質問 # 58**
What should organizations do with Key Risk Indicator KRI and Key Performance Indicator KPI data to facilitate decision making, and improve performance and accountability?

- A. Achieve, reset, and evaluate
- B. Collect, analyze, and report
- C. Prioritize, falsify, and report
- D. Challenge, compare, and revise

**正解：B**

解説：
KRIs and KPIs are only useful when they are handled as part of a disciplined measurement lifecycle. Cybersecurity governance guidance emphasizes three essential activities: collect, analyze, and report. Organizations must first collect KRI and KPI data consistently from reliable sources such as vulnerability scanners, SIEM logs, IAM systems, ticketing platforms, and asset inventories. Collection requires defined metric owners, clear definitions, standardized time windows, and data quality checks so results are comparable across periods and business units.
Next, organizations analyze the data to understand what it means for risk and performance. Analysis includes trending over time, comparing results to targets and thresholds, correlating indicators to business outcomes, identifying outliers, and determining root causes. For KRIs, analysis highlights rising exposure or control breakdowns such as increasing critical vulnerabilities beyond SLA. For KPIs, analysis evaluates operational effectiveness such as mean time to detect and mean time to remediate.
Finally, organizations report results to the right audiences with the right level of detail. Reporting supports accountability by assigning actions, tracking remediation progress, and escalating when thresholds are exceeded. It also supports decision making by showing where investment, staffing, or control changes will have the greatest risk-reduction and performance impact. The other options are not standard, auditable metric management activities and do not reflect the established lifecycle used in cybersecurity measurement programs.

**質問 # 59**
What is defined as an internal computerized table of access rules regarding the levels of computer access permitted to login IDs and computer terminals?

- A. Relational Access Database
- B. Access Control Entry
- C. Directory Management System
- D. Access Control List

**正解：D**

解説：
An Access Control List (ACL) is a structured, system-maintained list of authorization rules that specifies who or what is allowed to access a resource and what actions are permitted. In many operating systems, network devices, and applications, an ACL functions as an internal table that maps identities such as user IDs, group IDs, service accounts, or even device/terminal identifiers to permissions like read, write, execute, modify, delete, or administer. When a subject attempts to access an object, the system consults the ACL to determine whether the requested operation should be allowed or denied, enforcing the organization's security policy at runtime.
The description in the question matches the classic definition of an ACL as a computerized table of access rules tied to login IDs and sometimes the originating endpoint or terminal context. ACLs are central to implementing discretionary access control and are also widely used in networking (for example, permitting or denying traffic flows based on source/destination and ports) and file systems (controlling access to folders and files).
An Access Control Entry (ACE) is only a single line item within an ACL (one rule for one subject). A "Relational Access Database" is not a standard security control term for authorization tables. A "Directory Management System" manages identities and groups, but it is not the same as the enforcement list attached to a specific resource. Therefore, the correct answer is Access Control List.

**質問 # 60**
.....

IIBA-CCA実践教材は、すべての点で同様の製品よりも優れていると自信を持って伝えることができます。まず、ユーザーはIIBA-CCA試験準備を無料で試用して、IIBA-CCAスタディガイドをよりよく理解することができます。ユーザーが製品が自分に適していないことに気付いた場合、ユーザーは別の種類の学習教材を選択できます。ユーザーの選択を尊重し、ユーザーがIIBA-CCA実践教材を購入する必要があることを強制しません。ユーザーが適格なIIBA-CCA試験に合格できるように、ユーザーのすべての要件を可能な限り満たすことができます。