

実際試験を模擬するHITRUST CCSFP試験問題集のソフト版を紹介



2025年GoShikenの最新CCSFP PDFダンプおよびCCSFP試験エンジンの無料共有：<https://drive.google.com/open?id=1Pr7zcfT1ikPsbWxaANXIEyL4D0Kc2RBM>

もし、あなたはCCSFP試験に合格することを願っています。しかし、いい復習資料を見つけません。CCSFP復習資料はちょうどあなたが探しているものです。CCSFP復習資料は的中率が高く、便利で、使いやすく、全面的なものです。従って、早くCCSFP復習資料を入手しましょう！

当社GoShikenのCCSFP練習トレントは99%以上のパス保証を提供します。つまり、CCSFPの資料を真剣に検討し、提案を考慮に入れると、CCSFP証明書を確実に取得して目標を達成できます。一方、このコースを引き続き学習したい場合は、CCSFPテスト準備による充実したサービスをお楽しみいただけます。アフターサービスでは、1年以内に既存のCCSFP学習教材を更新し、複数の割引年。

>> CCSFP日本語版テキスト内容 <<

認定する-実際のなCCSFP日本語版テキスト内容試験-試験の準備方法 CCSFP勉強資料

GoShikenは君の成功のために、最も質の良いHITRUSTのCCSFP試験問題と解答を提供します。もし君はいささかな心配することがあるなら、あなたはうちの商品を購入する前に、GoShikenは無料でサンプルを提供することができます。あなたはGoShikenのHITRUSTのCCSFP問題集を購入した後、私たちは一年間で無料更新サービスを提供することができます。

HITRUST CCSFP 認定試験の出題範囲:

| トピック | 出題範囲 |
|--------|--|
| トピック 1 | <ul style="list-style-type: none">評価者の役割と責任の理解: この試験セクションでは、情報セキュリティマネージャーのスキルを測定し、HITRUST認定プロセスにおける評価者の責任を明確にします。コンプライアンス評価における独立性、客観性、そして専門的な行動の重要性を強調します。 |
| トピック 2 | <ul style="list-style-type: none">方法論の更新と強化: このセクションでは、情報セキュリティマネージャーのスキルを評価し、HITRUST方法論の最新情報を常に把握しておくことの重要性について説明します。これにより、受験者は新しい強化点を適用し、進化する標準に合わせて評価手法を調整できるようになります。 |
| トピック 3 | <ul style="list-style-type: none">評価範囲の設定に関する考慮事項: このセクションでは、情報セキュリティマネージャーのスキルを評価し、評価範囲を適切に定義する方法を説明します。受験者は、組織の規模、システム、規制要件が評価範囲の設定プロセスにどのような影響を与えるかを理解し、評価が正確かつビジネスニーズに適合していることを保証できます。 |
| トピック 4 | <ul style="list-style-type: none">HITRUSTスコアリングアプローチを用いたフレームワークコンプライアンス評価: この試験セクションでは、コンプライアンスアナリストのスキルを測定し、HITRUSTスコアリング手法の適用に焦点を当てます。スコアリングを用いてコンプライアンス成熟度を評価する方法を示し、専門家が複数の評価において一貫した結果解釈を行うのに役立ちます。 |

- HITRUST 品質保証の期待事項: この試験セクションでは、コンプライアンスアナリストのスキルを測定し、HITRUST が要求する品質基準を網羅します。評価が HITRUST の保証および信頼性基準を満たすことを保証するために、正確性、一貫性、および文書化に関する期待事項が強調されます。

HITRUST Certified CSF Practitioner 2025 Exam 認定 CCSFP 試験問題 (Q10-Q15):

質問 # 10

In an il assessment a Control Reference score of 62 would yield which result?

- A. A HITRUST certification
- B. A Control Reference gap
- C. A required CAP for all gaps within the associated Requirement Statements
- D. An optional CAP for all gaps within the associated Requirement Statements

正解: C

解説:

In an il assessment, scoring follows a pass/fail logic tied to CAP requirements. If a Control Reference scores below the defined threshold (typically 83 for il assessments), any gaps within its requirement statements must be addressed with a required Corrective Action Plan (CAP). A score of 62 is below the threshold, meaning it cannot be accepted without remediation. This ensures organizations remediate key cybersecurity hygiene gaps, even in a moderate assurance assessment. Optional CAPs are not used in il assessments, as the assurance program emphasizes mandatory remediation for below-threshold controls. Certification cannot be granted with unresolved required CAPs. Therefore, the correct outcome for a score of 62 in an il Control Reference is a required CAP.

References: HITRUST CSF Assurance Program - "il Assessment Scoring Rules"; CCSFP Practitioner Guide - "CAP Requirements in il Assessments."

質問 # 11

How many domains are there in an assessment?

正解:

解説:

19

Explanation:

The HITRUST CSF is structured into 19 domains that provide comprehensive coverage of information security and privacy practices.

These domains represent major categories of controls such as Information Security Management, Endpoint Protection, Network Security, Access Control, Configuration Management, Incident Management, and Data Protection.

Each domain contains multiple control references mapped to requirement statements, which are tailored to organizational and regulatory factors. This domain structure ensures that assessments address administrative, technical, and organizational safeguards consistently across industries. All assessment types—whether e1, il, or r2—utilize these 19 domains, although the number of requirement statements varies depending on the scope. The domain-based structure also supports HITRUST's mapping to authoritative sources like NIST, HIPAA, and ISO, ensuring consistency across compliance obligations.

References: HITRUST CSF Framework Overview - "Domain Structure"; CCSFP Study Guide - "The 19 Domains of the HITRUST CSF."

質問 # 12

When an implementation gap is remediated, what is the minimum number of days the control must operate before retesting? [0130]

- A. 60 Days
- B. 30 Days
- C. 90 Days
- D. Immediately

正解: A

解説:

For Implemented domain remediations, HITRUST requires 60 days of operation before retesting. This ensures the control is not only deployed, but also functioning effectively over time.

A 30-day threshold applies to Policy/Process, while Implemented requires longer to validate consistent application.

Extract Reference (HITRUST CSF Scoring & CAP Guidance [0130]):

Implementation gaps must show at least 60 days of operating effectiveness before retesting can validate remediation.

質問 # 13

Which AI models can be evaluated using the A1 Security Assessment?

- A. Back Propagation
- B. Generative
- C. Hodgkin-Huxley
- D. Predictive
- E. Rule-Based

正解: B、D、E

解説:

The A1 Security Assessment module evaluates the security, governance, and risk management of artificial intelligence models.

HITRUST specifies coverage for widely used model types, including:

* Predictive models, which forecast outcomes based on historical data (e.g., fraud detection, patient risk scoring).

* Generative models, which create new data outputs (e.g., AI image or text generators).

* Rule-based models, which use defined logic for decision-making.

The goal of the A1 assessment is to ensure that these AI models are developed, implemented, and monitored securely, with appropriate safeguards around data integrity, bias management, and model explainability.

Options like Hodgkin-Huxley (a neuroscience model) and Back Propagation (a training algorithm) are not types of AI models scoped by the A1 assessment. Instead, the A1 factor focuses on applied model categories used in operational environments.

References: HITRUST A1 Security Assessment Guide - "Applicable AI Models"; CCSFP Practitioner Training - "AI Risk and Model Categories."

質問 # 14

An r2 Requirement Statement that scores at a 37 would yield which result?

- A. Function Gap
- B. Gap with possible required CAP
- C. Risk Acceptance
- D. No Gap
- E. HITRUST Certification

正解: B

解説:

HITRUST uses a scoring scale from 0 to 100, with categories for Fully Compliant, Mostly Compliant, Partially Compliant, Somewhat Compliant, and Non-Compliant. A score of 37 falls into the "Somewhat Compliant" category. This reflects significant weaknesses in Policy, Procedure, or Implementation maturity levels. Such a low score indicates a gap that must be addressed.

Depending on whether the control is required for certification, HITRUST may require a Corrective Action Plan (CAP). CAPs are required when certification-critical controls score below thresholds (e.g., Implementation not at 100% where required).

Therefore, a Requirement Statement score of 37 would be treated as a gap with a possible required CAP, depending on its criticality within the certification process.

References: HITRUST CSF Scoring Rubric - "Compliance Categories and CAP Triggers"; CCSFP Study Guide - "Requirement Scoring Outcomes."

質問 # 15

.....

