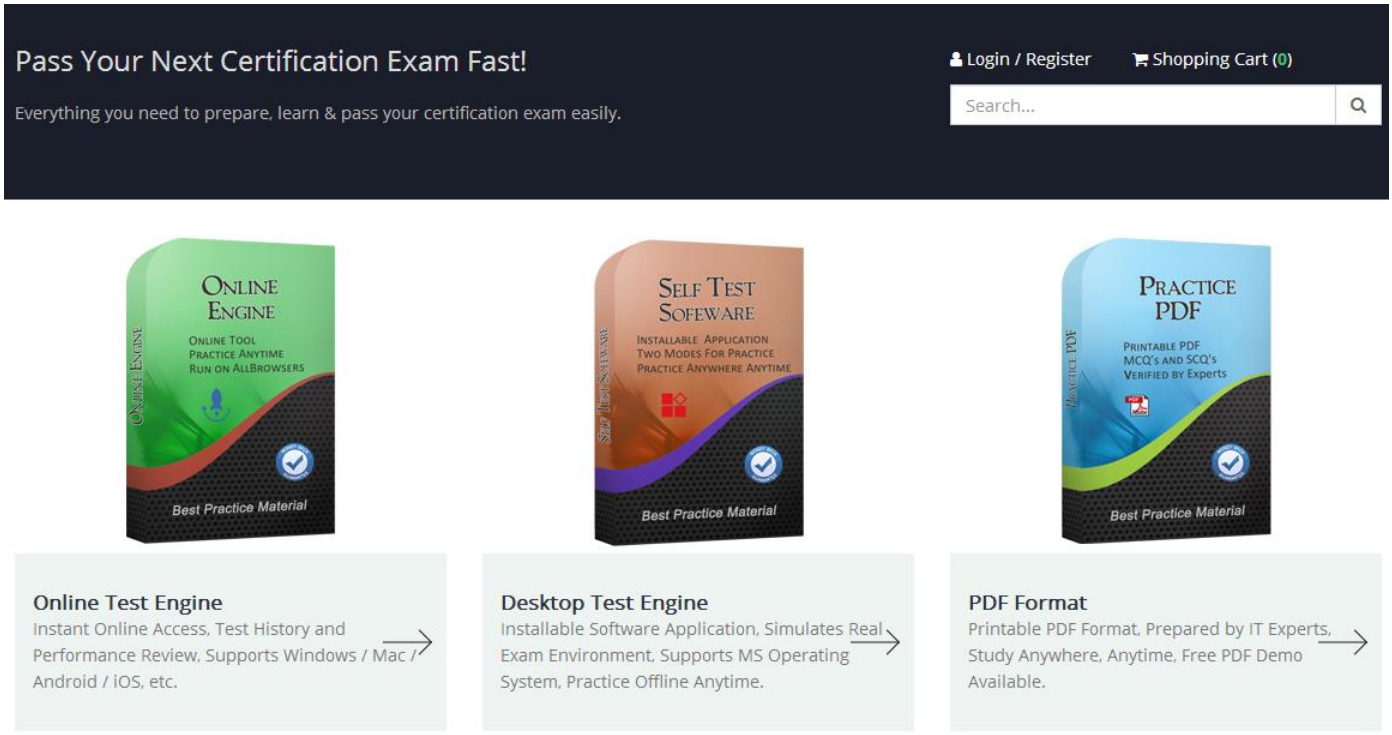
Actual4Labs



Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.actual4labs.com

Excellent Quality Exam Dumps Questions Never Let You down - Actual4Labs

Exam : **CCSFP**

Title : Certified CSF Practitioner 2025 Exam

Vendor : HITRUST

Version : DEMO

NO.1 Upon submission of an assessment object by the assessor, how many days does HITRUST take to either accept or reject the assessment?

A. 1-2 days

B. 3-5 days

C. 7 days

D. 14 days

Answer: B

Explanation:

When an assessor submits a validated assessment object to HITRUST, the QA intake process begins. HITRUST typically takes 3-5 business days to complete an initial review and decide whether to accept the submission into the QA pipeline or reject it due to deficiencies (such as missing evidence, incomplete CAPs, or improper scoping). Acceptance at this stage does not mean certification-it simply indicates that the assessment meets the minimum requirements to enter QA. If rejected, the assessor must correct the issues before resubmission. The 3-5 day timeframe ensures efficiency while maintaining rigor in intake quality checks.

References: HITRUST Assurance Program Requirements - "Submission Review and Intake Timeline"; CCSFP Study Guide - "Assessment Submission to QA."

NO.2 How is the sample of Requirement Statements within an interim assessment selected for testing?

A. By the assessor personnel

B. By client personnel

C. Randomly by the MyCSF tool

D. Any with associated gaps

E. Any with required CAPs

Answer: C D E

Explanation:

During an interim assessment for r2 certifications, only a subset of Requirement Statements is retested. This sample is not determined manually by assessors or clients but is systematically generated by MyCSF. The tool ensures randomness and fairness while including mandatory items such as:

* Requirement Statements with open gaps from the prior validated assessment.
* Requirement Statements with active Corrective Action Plans (CAPs).
* A random selection of additional requirements to confirm continued control performance.

This approach balances efficiency and assurance. It ensures that areas of previously identified weakness are re- examined while still sampling across the broader control set. By automating sample selection, HITRUST prevents bias and ensures consistency across interim reviews.

s: HITRUST Interim Assessment Guide - "Sample Selection for Interims"; CCSFP Practitioner Guide - "Interim Testing and MyCSF Sampling Process."

NO.3 For an r2 assessment, to obtain a Validated Report with Certification, each domain must score at least a 71 or higher.

A. True

B. False

Answer: A
Explanation:
HITRUST requires that each of the 19 domains achieve a minimum score of 71 for an organization to qualify for r2 certification. This threshold ensures that entities maintain a consistent level of maturity across all control areas, rather than excelling in some while neglecting others. The 71 threshold is calculated from the weighted average of requirement statements within a domain, factoring in Policy, Procedure, and Implementation maturity scores (with Measured and Managed as applicable). If any domain falls below 71, the assessment may still produce a validated report, but it will not result in certification. This strict requirement highlights HITRUST's emphasis on balanced coverage across all areas of security and privacy.
References: HITRUST CSF Scoring Rubric - "Certification Thresholds"; CCSFP Practitioner Guide - "Minimum Domain Score Requirements."

NO.4 In an r2 assessment, if the responsibility for a Requirement Statement is split between the client and one or more service providers, should only the service provider scores be used?
A. No, take a blended approach to scoring and consider the responsibilities for all parties involved
B. No, you should only score the client's portion of the responsibility
C. No, you should mark this Requirement Statement N/A as it has been outsourced
D. No, because this never happens
E. Yes, these are the most important scores
Answer: A
Explanation:
When a Requirement Statement's responsibility is shared between a client and service providers (e.g., cloud vendors or managed security providers), HITRUST requires a blended scoring approach. Assessors must evaluate all parties' contributions and assign a composite score that reflects the total control environment.
This prevents organizations from over-relying on inherited provider scores without demonstrating their own responsibilities (e.g., configuration, monitoring). It also prevents dismissing requirements as N/A since partial responsibility still exists. By combining the provider's validated assessment results with the client's implementation evidence, HITRUST ensures a complete and accurate reflection of risk. Sole reliance on provider scores would overlook gaps in client-side processes.
References: HITRUST Inheritance Guidance - "Blended Scoring of Shared Responsibility"; CCSFP Practitioner Guide - "Scoring Split Responsibility."

NO.5 How large would the sample size be for a manual control with a population of 56 unique items?
A. 5
B. 8
C. 6
D. 25
E. 56
Answer: B
Explanation:
HITRUST provides sampling guidance in the CSF Assessment Methodology and scoring rubric for manual controls. Sample sizes are determined by the population of items and the control's

frequency. For a population of 56 items, the expected sample size is 8, following HITRUST's defined sampling table. This approach is based on statistical sampling principles but simplified for consistent assessor use. The sample must be randomly selected and representative of the entire population to avoid bias. Larger populations require larger sample sizes, but at certain thresholds, the increase is incremental. For example, a population between 26-100 items requires a sample size of 8. This ensures sufficient testing coverage without requiring a full census.
Therefore, the correct sample size for 56 items is 8.
References: HITRUST CSF Scoring Rubric - "Sampling Requirements for Manual Controls"; CCSFP Study Guide - "Sampling by Population Size."

NO.6 The assessor plans to test a population in a file, and they want to pick every 100th item. Which of the recognized sampling methodologies would best describe the sample that will be pulled?
A. Systematic/Interval
B. Judgmental
C. Random
D. Haphazard
Answer: A
Explanation:
Systematic/Interval sampling is a recognized statistical methodology where items are selected at regular intervals from an ordered population. For example, selecting every 100th transaction, log entry, or user account from a file. This approach provides coverage across the dataset while being more efficient than random sampling. HITRUST accepts systematic sampling as long as the population is not ordered in a way that introduces bias (e.g., chronological logs where every 100th entry might reflect similar conditions). By contrast, random sampling requires a truly random number generator, judgmental relies on assessor discretion, and haphazard lacks any structured methodology. For this scenario, selecting every 100th item is clearly Systematic/Interval sampling.
References: HITRUST Scoring Rubric - "Sampling Techniques"; CCSFP Study Guide - "Recognize
d Sampling Methodologies."

NO.7 A validated assessment is only available to organizations after performing a readiness assessment. [0020]
A. True
B. False
Answer: B
Explanation:
A validated assessment does not require a readiness assessment as a prerequisite.
A Readiness Assessment is optional and intended to help organizations self-identify gaps before a validated assessment.
A Validated Assessment involves an independent HITRUST Authorized External Assessor validating evidence and submitting results to HITRUST for quality assurance and potential certification.
Many organizations choose to do a readiness assessment first, but it is not mandatory.
Extract Reference (CCSFP Study Guide & HITRUST CSF Assurance Program [0020]):
Organizations may perform a readiness assessment prior to a validated assessment to identify gaps, but it is not required; validated assessments can be performed independently.

NO.8 MyCSF analytics can be used to visualize data within an assessment object as well as across all assessment objects within an organization.

A. True

B. False

Answer: A

Explanation:

MyCSF Analytics is a feature that allows organizations to create dashboards, charts, and reports from their assessment data. Analytics can be applied within a single assessment object to track scoring, evidence linkage, CAPs, and requirement coverage. Additionally, analytics can be applied across multiple assessments (e.g., e1, i1, and r2 objects) within the same subscriber organization. This cross-assessment capability is especially valuable for large enterprises performing multiple assessments for different business units or regulatory drivers. It enables comparisons, benchmarking, and enterprise-wide risk visibility. The analytics feature enhances MyCSF's role as not only an assessment tool but also a continuous risk management platform, giving organizations insight into trends and performance over time.

References: MyCSF User Guide - "Analytics and Reporting Functions"; CCSFP Practitioner Guide - "Using MyCSF Analytics Across Assessments."

NO.9 The AI Risk Assessment compliance factor is used to obtain the HITRUST AI Security Certification. [0007]

A. True

B. False

Answer: B

Explanation:

The AI Risk Assessment compliance factor is used to scope AI-related controls in assessments. However, the HITRUST AI Security Certification requires assessment of AI Security requirements, not just the AI Risk Assessment factor.

Thus, the statement is incorrect.

Extract Reference (HITRUST AI Security Factor Guidance [0007]):

The AI Risk Assessment factor scopes AI-related controls but does not by itself equate to AI Security Certification.

NO.10 Which assessment type is the most tailorable to an organization's risk profile?

A. i1

B. r2

C. Interim

D. e1

E. Bridge

Answer: B

Explanation:

The r2 assessment is the most risk-tailorable of all HITRUST assessment types. Unlike the standardized e1 and i1 assessments, which are designed for essential or moderate assurance, the r2 adapts dynamically based on organizational, technical, compliance, and operational risk factors. For example, the number of users, systems, or internet-facing components directly impacts the number and type of requirement statements.

Regulatory drivers such as HIPAA, PCI-DSS, or GDPR also add requirements, ensuring the assessment aligns with the entity's unique obligations. This tailoring ensures that organizations with higher risk exposure face more stringent testing, while lower-risk entities are not overburdened with unnecessary controls. Neither interim assessments nor bridge certificates are tailorable-they are point-in-time processes tied to existing validated assessments.
References: HITRUST CSF Methodology - "Risk-Based Tailoring"; CCSFP Study Guide - "Why r2 is th e Most Customizable Assessment."

NO.11 All assessment domains are updated with additional requirements when the AI Security factor is selected.

A. True

B. False

Answer: B

Explanation:
When the AI (A1) Security factor is selected during scoping, HITRUST does not add requirements across all
19 domains. Instead, it introduces specific requirement statements relevant to AI risks, such as data integrity, model governance, algorithm transparency, and monitoring. These requirements are mapped to domains most impacted by AI operations, like Information Protection, Risk Management, and Data Privacy. Domains unrelated to AI (for example, Facilities Security or Environmental Safeguards) may not receive any new requirements. This selective approach ensures that AI risk factors are incorporated appropriately without overloading domains unnecessarily. Thus, it is inaccurate to state that every domain is updated with AI- related requirements.
References: HITRUST A1 Security Assessment Guide - "Domain Applicability"; CCSFP Study Guide - "A I- Specific Requirement Mapping."

NO.12 When are HITRUST Assurance Advisories (HAA) posted? [0167]

A. There is no formal schedule for issuing Assurance Advisories

B. Annually

C. Quarterly

D. Monthly

Answer: A

Explanation:
HITRUST Assurance Advisories (HAAs) are issued when necessary to communicate important updates, clarifications, or changes impacting the CSF Assurance Program. These advisories are not bound to a fixed schedule (monthly, quarterly, or annually), but rather published as needed.
Extract Reference (HITRUST CSF Assurance Program, CCSFP Content [0167]):
There is no formal schedule for issuing HITRUST Assurance Advisories; they are published on an as-needed basis to communicate relevant updates.
Correct response: There is no formal schedule.

NO.13 When considering third-party reports for reliance, what must be included in the report? (Select all that apply)

A. Description of scope

B. Completed remediation for testing exceptions

C. List of procedures performed
D. Executive summary
E. Conclusions reached for each test
Answer: A C E
Explanation:
When relying on third-party reports (such as SOC 2 reports) to satisfy HITRUST requirements, only reports with sufficient detail can be used. HITRUST requires:
* A clear description of scope (A) to confirm applicability to the assessed environment.
* A list of procedures performed (C) so assessors can evaluate whether testing covered relevant controls.
* Conclusions reached for each test (E) to provide assurance about the effectiveness of tested controls.
While an executive summary may be helpful for context, it lacks sufficient detail to serve as valid reliance evidence. Similarly, "completed remediation" of exceptions (B) is not required; rather, the report must document exceptions transparently. Assessors remain responsible for verifying that reliance reports are current, relevant, and issued by qualified independent auditors.
References: HITRUST External Reliance Guidance - "Requirements for Third-Party Reports"; CCSFP Study Guide - "Use of SOC 2 and Similar Reports."

NO.14 A validated assessment may lead to either a validated report or a validated report with certification.
A. True
B. False
Answer: A
Explanation:
Validated assessments undergo QA by HITRUST after submission by the assessor. The outcome can be either:
* A Validated Report - issued if the assessment is complete but certification thresholds (e.g., domain scores #71 for r2) are not met. This report still provides assurance to relying parties by confirming independent validation, even without certification.
* A Validated Report with Certification - issued when all certification criteria are met, including minimum domain scores and interim assessment requirements for multi-year validity.
This distinction allows HITRUST to provide value even to organizations that fall short of certification, by documenting their current control maturity and gaps. Organizations can use the validated report as a roadmap to remediate deficiencies and pursue certification in the future.
References: HITRUST Assurance Program Overview - "Validated Reports and Certification"; CCSFP Study Guide - "Assessment Outcomes."