HITRUST CCSFP Practice Questions

Shared by Morton on 06-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following are appropriate types of inheritance within MyCSF? (Select all that apply) [0061]

Options:

A- Cross Organizational
B- Bi-lateral
C- Internal
D- External

P2P exams

Answer:

A, C, D

Explanation:

In HITRUST MyCSF, inheritance allows organizations to leverage control implementations from other entities or internal departments to reduce redundancy and streamline assessments.

Cross Organizational inheritance Accepted, allows borrowing controls from a trusted external organization (e.g., cloud provider).

Internal inheritance Accepted, allows reuse of controls across internal business units or shared services.

External inheritance Accepted, typically when outsourcing to a vendor that provides evidence.

Bi-lateral inheritance Not recognized by HITRUST, as inheritance flows one way only (from provider to relying party).

Extract Reference (HITRUST MyCSF User Guide, CCSFP Program Objectives):

Appropriate inheritance types include cross organizational, internal, and external. Bi-lateral inheritance is not supported in MyCSF, as inheritance is directional and validated only from provider to consumer.

Question 2

Question Type: MultipleChoice

To perform a rapid assessment, the assessment and/or insights report must each contain more than 60 requirements.

Options:

A- True
B- False

Answer:

B

P2P exams

Explanation:

HITRUST offers Rapid Assessments as a lightweight reporting option for organizations and their relying parties. These assessments provide high-level visibility without requiring large numbers of requirements. In fact, a Rapid Assessment may contain fewer than 60 requirement statements depending on scoping and factors selected. There is no requirement that an assessment or insights report exceed 60 requirements to qualify as a rapid assessment. Instead, the determination is based on the selected assessment type (e1, i1, or targeted factors) and whether the output is requested in ''rapid'' format. This flexibility allows small organizations or specific use cases to leverage HITRUST without unnecessary burden.

Question 3

Question Type: MultipleChoice

P2P exams

Where in MyCSF can the CSF framework be browsed?

Options:

A- Home
B- Tasks
C- Administration
D- Reference Library
E- Search

Answer:

D

Explanation:

In MyCSF, the Reference Library is the designated area where users can browse the entire HITRUST CSF framework. This includes domains, control references, requirement statements, and illustrative procedures. The Reference Library provides an organized view of the framework that is independent of any active assessment object. This feature is especially useful for entities preparing for scoping, training, or developing internal control mappings. While the Search function allows keyword lookups and the Home page provides general dashboards, only the Reference Library offers the structured, domain-by-domain framework view. This ensures that users can review and study the CSF in its entirety before or during assessment preparation, without needing to navigate through specific assessment objects.

P2P exams

Question 4

Question Type: MultipleChoice

Measured and Managed Maturity Levels can be scored for some, but not all, requirements in an r2 assessment object.

Options:

A- True
B- False

Answer:

A

P2P exams

Explanation:

The HITRUST scoring methodology uses five maturity levels: Policy, Procedure, Implemented, Measured, and Managed. However, not every requirement statement includes Measured and Managed maturity elements. These two levels are applied selectively, particularly to requirements that lend themselves to performance monitoring and ongoing governance. For example, requirements involving logging, monitoring, and reporting often include ''Measured'' and ''Managed'' dimensions, while policy-only requirements may not. In r2 assessments, assessors should review the applicable requirement statements in MyCSF to see which maturity levels are required. This ensures that maturity scoring is accurate and aligned with HITRUST's intent. Therefore, the statement that Measured and Managed can be scored for some but not all

requirements in r2 is True.

Question 5

Question Type: MultipleChoice

If the client and the External Assessor disagree on assessment scope, HITRUST will determine the final scope. [0027]

Options:

A- True
B- False

Answer:

B

Explanation:

HITRUST does not determine scope in disputes between clients and assessors.

The organization (subscriber) ultimately owns responsibility for defining and attesting to the assessment scope.

The External Assessor is responsible for verifying that the defined scope is reasonable, complete, and appropriate.

HITRUST only reviews submitted assessments for quality assurance but does not directly arbitrate scope disagreements.

Extract Reference (HITRUST CSF Assurance Program, CCSFP Guidance [0027]):

Subscribers determine scope; External Assessors validate scope appropriateness. HITRUST does not dictate or resolve scope disputes.

Question 6

Question Type: MultipleChoice

Using only the information from the chart and question below, please answer:

This assessment will be able to achieve certification. [0192]

Options:

A- True
B- False

Answer:

B

Explanation:

:

Certification requires all Requirement Statements to meet the 62.5% threshold.

From the chart:

''The Privacy Officer...'' scored 42, below 62.5.

''Antivirus clients have...'' scored 62, also below 62.5.

Because there are Requirement Statements below threshold, the assessment will contain Required CAPs, and certification cannot be awarded until remediation.

Extract Reference (HITRUST CSF Scoring Methodology [0192]):

Certification requires all Requirement Statements to meet the minimum scoring threshold; scores below 62.5 prevent certification.

Question 7

Question Type: MultipleChoice

Management has asked you to scope out an assessment including your entire network. What are some examples you may see listed as a primary scoping component?

Options:

A- Hypervisor
B- Server
C- Oracle database
D- Smoke detectors
E- Network attached storage device

Answer:

A, B, C, E

Explanation:

Primary scoping components are systems, applications, and infrastructure directly involved in processing, storing, or transmitting sensitive information. Examples include hypervisors (supporting virtualized systems), servers (hosting applications and data), databases like Oracle (storing structured data), and network attached storage (NAS) devices (storing files). These are all core elements of an IT environment subject to assessment. By contrast, smoke detectors are physical safety devices, not considered primary scoping components for HITRUST. Physical safeguards like detectors may fall under facility security, but they are not tested as primary IT components. Proper identification of primary scoping components is critical to defining the assessment boundary and ensuring appropriate requirements are applied.

Question 8

Question Type: MultipleChoice

An r2 certification is good for how many years?

Options:

A- Two years provided an interim assessment is performed, all CAPs have been remediated, and all N/As discharged
B- Two years provided an interim assessment is performed and interim requirements are met
C- Two years regardless
D- Until there has been a significant change in the in-scope environment

Answer:

B

Explanation:

An r2 certification is valid for two years, but only if an interim assessment is performed at the one-year mark and interim requirements are met. The interim assessment ensures that the organization continues to maintain its controls, remediate CAPs, and discharge any pending N/A justifications. If an interim is not completed or requirements are not met, the certification can lapse. Unlike option A, remediation of all CAPs and N/As is not required before certification is maintained, though CAP progress must be monitored. Certification is not automatically valid for two years (option C), nor is it indefinite (option D). Thus, the correct answer is that certification is valid for two years provided interim requirements are met.

Question 9

Question Type: MultipleChoice

The Certified CSF Practitioner (CCSFP) designation is good for how many years?

Options:

A- 4 years
B- 1 year provided the CHQP has been completed
C- 3 years provided annual refresher training has been completed
D- 2 years with no refresher training

Answer:

D

Explanation:

The Certified CSF Practitioner (CCSFP) designation, awarded through HITRUST Academy, is valid for two years from the date of certification. During this period, practitioners are recognized as trained professionals qualified to assist organizations in implementing, preparing for, and supporting HITRUST CSF assessments. Unlike certifications in some other frameworks, CCSFP does not require annual refresher training for continued validity. After the two-year period, practitioners must renew their certification, typically by retaking the CCSFP course or completing updated training to ensure knowledge of the latest HITRUST CSF version and Assurance Program changes. The two-year cycle aligns with HITRUST's update cadence, ensuring practitioners remain current with evolving regulatory mappings, control requirements, and scoring methodology.

Question 10

Question Type: MultipleChoice

When considering third-party reports for reliance, what must be included in the report? (Select all that apply)

Options:

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.

Question 11

Question Type: MultipleChoice

To place reliance on a point-in-time assessment report, the issue date must be within two years from the assessment fieldwork start date. [0078]

Options:

A- True
B- False

Answer:

B

P2P exams

Explanation:

Comprehensive and Detailed

According to the HITRUST CSF Assurance Program, the reliance period for a point-in-time assessment is one year (12 months) from the assessment report date.

The statement claims a two-year validity, which is incorrect.

Reliance beyond one year would require an updated assessment or interim assessment for assurance continuity.

Extract Reference (HITRUST CSF Assurance Program, CCSFP Objectives [0078]):

Point-in-time reports can only be relied upon if issued within one year from the assessment start date; two years is not permitted.

P2P exams

Question 12

Question Type: MultipleChoice

Insights Reports provide a more comprehensive review of authoritative sources than a standard e1 report. [0042]

Options:

A- True
B- False

Answer:

A

Explanation:

Insights Reports are designed to provide deeper analytics and benchmarking than standard e1 reports.

They expand visibility into authoritative sources, industry comparisons, and organizational insights beyond what a basic e1 delivers.

Extract Reference (HITRUST Assurance Program Reporting [0042]):

Insights Reports provide a more comprehensive analysis, including authoritative source mapping and benchmarking, beyond the standard e1 report.

To Get Premium Files for CCSFP Visit

https://www.p2pexams.com/products/ccsfp

For More Free Questions Visit

https://www.p2pexams.com/hitrust/pdf/ccsfp

