DUMPSBOSS.

Certified CSF Practitioner 2025 Exam

HITRUST CCSFP

Version Demo

Total Demo Questions: 16

Total Premium Questions: 161

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, HITRUST CSF	15
Topic 2, HITRUST CSF Assessment	115
Topic 3, HITRUST CSF Reporting	10
Topic 4, HITRUST CSF Certification	21
Total	161

QUESTION NO: 1 - (SIMULATION)

How many domains are there in an assessment?

ANSWER: See the explanation for the answer

Explanation:

Answer: 19 domains.

A HITRUST CSF assessment is organized across 19 control domains. The applicable requirement statements within those domains are tailored based on the assessment type and organizational factors.

QUESTION NO: 2

Select the four general risk factor categories used when scoping r2 assessments.

A. Technical

B. General

C. Organizational

D. Compliance

E. Operational

F. Privacy

G. Geographic

ANSWER: A C D G

Explanation:

HITRUST r2 assessment scoping uses general risk factors to tailor the assessment's requirement statements and implementation levels to the assessed entity and the systems in scope. The four general categories are Technical, Organizational, Regulatory (represented here by "Compliance"), and Geographic. Technical factors address the technology environment and characteristics that influence control complexity. Organizational factors account for entity characteristics relevant to the assessment context. Regulatory or compliance factors identify applicable legal, regulatory, and contractual obligations that influence the authoritative sources and requirements included in the assessment. Geographic factors account for the jurisdictions in which the organization operates or processes relevant information, since jurisdictions can create distinct legal and regulatory obligations. Together, these factors support a risk-based, appropriately tailored r2 assessment rather than a uniform set of requirements for every organization and system. HITRUST describes its CSF and assessment approach as a comprehensive, risk-based framework that can incorporate multiple authoritative sources and organizational contexts. See the HITRUST CSF overview and the HITRUST Assurance Intelligence Engine overview.

QUESTION NO: 3

The HITRUST CSF is built upon the following model: [0134]

A. Control Objectives, Control References, COBIT Controls

B. Functions, Categories, Sub-Categories

C. Control Categories, COBIT controls, Implementation levels

D. Control Categories, Control Objectives, Control References

ANSWER: D

Explanation:

Control Categories, Control Objectives, Control References is correct because it describes the hierarchical structure used to organize the HITRUST CSF. Control Categories are the highest-level domains that group related security, privacy, and risk-management subject matter. Within each category, Control Objectives state the intended security or assurance outcomes. Control References then provide the specific, assessable control requirements and implementation considerations used to evaluate whether those objectives are met. This hierarchy supports traceability: an assessor or control owner can connect a detailed requirement to its objective and the broader category it supports. HITRUST also tailors requirements using factors such as organizational, system, and regulatory risk, but that tailoring occurs within this structured control model rather than replacing it. The model enables HITRUST to map authoritative sources and industry requirements into a consistent, certifiable framework while retaining actionable control-level detail. HITRUST describes the CSF as a comprehensive, certifiable framework with controls organized to support scalable assurance and risk management. See the HITRUST CSF overview and HITRUST's CSF resources page for framework information and documentation access.

QUESTION NO: 4

Can multiple assessments be performed on your organization simultaneously?

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. HITRUST assessments are managed as distinct assessment engagements, each with its own defined scope, assessment object, requirements, evidence, testing activities, and reporting workflow. An organization is therefore able to conduct multiple assessments concurrently when it has separate assurance needs—for example, assessments covering different systems, business units, legal entities, customers, or service offerings. Each engagement must still be planned and governed appropriately so that its scope is clear, the relevant inherited controls and shared services are identified, evidence is mapped to the correct assessment, and the applicable HITRUST assessment and quality-assurance processes are followed. Running assessments at the same time can help an organization align assurance work with customer commitments, certification timelines, or differing risk profiles without treating the entire enterprise as a single, inseparable assessment scope. HITRUST's assurance approach is designed around a tailored, risk-based assessment process rather than a one-size-fits-all organizational review. Additional information on HITRUST assurance services and the HITRUST CSF is available at HITRUST Assurance and HITRUST CSF.

QUESTION NO: 5

Before finalizing an assessment object, Client Management wants to compare proposed scoping scenarios without changing the existing object. Which two results can be obtained by using Preview Profile? (Select two)

A. Comparing the Requirement Statement counts produced by different factor selections

B. Submitting the assessment for HITRUST quality assurance

C. Evaluating possible scope configurations without updating the assessment object

D. Removing authoritative sources from the assessment object

E. Automatically changing the current assessment profile

ANSWER: A C

Explanation:

Comparing the Requirement Statement counts produced by different factor selections and **evaluating possible scope configurations without updating the assessment object** are correct. Preview Profile supports planning by allowing

users to model alternative scoping selections and understand their likely impact before formally changing the assessment configuration.

Preview Profile does not submit an assessment for validation, remove authoritative sources, or change the current assessment object automatically. Those activities are separate from the planning function provided by the preview capability.

QUESTION NO: 6

The process of testing Requirement Statements within the HITRUST CSF includes: (Select all that apply) [0026]

A. Interviewing of organizational personnel

B. Remediating deficient controls

C. Sampling populations

D. Examination of documentation

E. Testing of the technical implementation

ANSWER: A C D E

Explanation:

Testing HITRUST CSF Requirement Statements uses multiple assurance procedures to obtain sufficient, appropriate evidence that implemented controls are designed and operating effectively. Interviewing of organizational personnel is included because discussions with control owners and other relevant personnel help the assessor understand how a control operates in practice, identify responsible roles, and corroborate evidence obtained through other procedures. Sampling populations is included when a requirement is expected to operate repeatedly over a defined period; representative samples allow testing of whether performance was consistent rather than limited to a single occurrence. Examination of documentation includes reviewing policies, procedures, tickets, approvals, logs, reports, configurations, and other records that demonstrate control implementation and operation. Testing of the technical implementation is also a core procedure where a requirement involves technology: the assessor may inspect system settings, security configurations, access-control behavior, or generated evidence to validate the implementation directly. Together, these procedures support evidence-based assessment of requirement statements and align with HITRUST's expectation that validated assessments use appropriate testing methods and evidence. HITRUST describes its assessment and assurance approach in its HITRUST CSF overview and provides assessor resources through the HITRUST Assessor Program.

QUESTION NO: 7

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: B

Explanation:

False is correct. For HITRUST r2 certification, the applicable minimum domain score is 62, not 71. An r2 Validated Assessment is a comprehensive, risk-based assessment using the HITRUST CSF, and certification is issued only after the assessment and the external assessor's work have successfully completed HITRUST's quality-assurance review. The score requirement is evaluated at the domain level: the assessed organization must meet the certification threshold in every applicable assessment domain. Therefore, describing 71 as the required minimum for each domain inaccurately states the r2 certification criterion. HITRUST uses defined scoring and quality-assurance processes to ensure a certification represents a consistent level of implemented, measured, and managed security and privacy controls across the assessed scope. The resulting HITRUST r2 Validated Report with Certification provides reliance-oriented assurance to stakeholders, subject to the report scope, validity period, and any stated considerations. See HITRUST's overview of its assurance programs at HITRUST CSF and its resource materials at HITRUST Resource Center.

QUESTION NO: 8

What are HITRUST Assurance Advisories designed to provide? (Select all that apply) [0051]

A. Updates related to the HITRUST Assurance Program

B. List of all new and updated authoritative sources associated with a framework version update

C. End-of-Life progression for older framework versions

D. Solicitations for assessor input

E. All of the above

ANSWER: A B C D E

Explanation:

HITRUST Assurance Advisories are formal program communications intended to keep the assurance ecosystem informed about changes that affect use of the HITRUST CSF and the HITRUST Assurance Program. Accordingly, they provide updates related to the HITRUST Assurance Program, including operational or programmatic information relevant to organizations and Authorized External Assessors. They can also identify new and updated authoritative sources associated with a framework version update, helping stakeholders understand changes to the source material that informs CSF requirements and assessment content.

Advisories further communicate end-of-life progression for older framework versions so organizations can plan migrations, assessment timing, and use of supported versions. HITRUST may also use these communications to solicit assessor input, enabling feedback from practitioners who apply the framework and assurance methodology. Because each listed purpose is within the scope of these advisories, “All of the above” is also correct. These communications support consistent implementation and governance across the HITRUST assurance ecosystem. See HITRUST’s Assurance Program overview and its HITRUST CSF information page.

QUESTION NO: 9

Under which version of the CSF did the framework go industry agnostic and HIPAA became its own regulatory factor?

A. v9.2

B. v9.3

C. v9.0

D. v9.4

E. v9.1

ANSWER: C

Explanation:

v9.0 is correct. HITRUST CSF version 9.0 marked the framework’s transition from a model strongly associated with healthcare to a broadly applicable, industry-agnostic assurance framework. This evolution enabled organizations in sectors such as financial services, technology, manufacturing, and government to use a common control framework while tailoring requirements to their own risk, regulatory, and business contexts. As part of that change, HIPAA was separated from the universally applicable baseline and treated as a distinct regulatory factor. This allows HIPAA-related requirements to be incorporated when they are relevant to the assessed organization’s scope, rather than making them implicit for every organization using the CSF. The approach supports HITRUST’s core model of producing a tailored assessment by considering organizational, system, regulatory, and threat factors while retaining a consistent, certifiable control framework. HITRUST describes the CSF as a comprehensive framework that can be tailored across industries and regulatory environments; see the HITRUST CSF overview and the HITRUST assessment and certification overview.

QUESTION NO: 10

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:

There is no formal schedule for issuing Assurance Advisories. HITRUST Assurance Advisories are published when HITRUST needs to communicate timely information relevant to the CSF Assurance Program, such as program updates, clarifications, changes to assessment or reporting expectations, or other information that affects authorized external assessors and organizations using HITRUST assurance services. Because the subject matter and urgency of these communications can vary, a fixed monthly, quarterly, or annual publication cycle would not ensure that important guidance reaches stakeholders at the appropriate time. Practitioners should therefore monitor HITRUST program communications and the resources available through HITRUST rather than expecting advisories on a recurring calendar date. This approach supports the assurance program's goal of keeping assessment participants aligned with current requirements and operational guidance as those needs arise. HITRUST describes its assurance offerings and associated program resources at https://hitrustalliance.net/assurance-services. Additional information on the HITRUST CSF and assurance ecosystem is available at https://hitrustalliance.net/hitrust-csf.

QUESTION NO: 11

An organization has two assessment objects that both require the same approved access-control policy as evidence. Which two actions best support efficient evidence reuse in MyCSF? (Select two)

A. Store the approved policy in the document repository

B. Upload a separate duplicate of the policy for every assessment object

C. Use the repository document for each relevant assessment object

D. Delete the repository document after linking it to one assessment object

E. Treat the policy as sufficient evidence of implementation without testing

ANSWER: A C

Explanation:

Store the approved policy in the document repository and **use the repository document for each relevant assessment object** are correct. The document repository centralizes supporting documentation and enables appropriate reuse across multiple assessment objects, reducing unnecessary duplication while maintaining evidence consistency.

Creating separate duplicate uploads for each assessment object is not necessary when the same document is applicable. Deleting the original document after associating it with an assessment would undermine evidence availability. A repository document also does not eliminate the need to evaluate whether the policy is relevant, current, and supported by implementation evidence for each Requirement Statement.

QUESTION NO: 12

Control Objectives are a statement of the desired result or purpose to be achieved by implementing control procedures into a particular process.

A. True

B. False

ANSWER: A

Explanation:

True is correct. In the HITRUST CSF, control objectives express the intended purpose or outcome that an organization seeks to achieve within a process or security domain. They establish the result that controls are meant to support, rather than functioning as the detailed, testable activities used to implement that result. Control requirements and their associated implementation specifications provide the more specific direction for policies, procedures, configurations, and operational practices that an organization can use to satisfy the objective. This outcome-focused structure helps organizations understand the security, privacy, or risk-management purpose behind the controls they implement and assess. It also supports HITRUST's risk-based, scalable approach: organizations can tailor implementation according to applicable regulatory factors, organizational characteristics, and risk while remaining focused on achieving the stated control objective. HITRUST describes its CSF as a comprehensive, certifiable framework that harmonizes authoritative sources and enables organizations to manage information risk through defined, assessable control requirements. The distinction between an objective—the desired result—and the procedures used to attain it is therefore fundamental to interpreting and applying the framework. See the HITRUST CSF overview and the HITRUST CSF Certification information.

QUESTION NO: 13

An organization has identified a number of components needed for an assessment. These components cover systems/applications for customers in the states of Massachusetts and Nevada. Assuming management wants corresponding regulatory factors to be included in their assessment, which regulatory factors would apply?

(Select all that apply)

A. State of Massachusetts Data Protection Act

B. CMS Minimum Security Requirements (High)

C. State of Nevada Security of Personal Information Requirements

D. Texas Health and Safety Code

E. Subject to De-ID Requirements

ANSWER: A C

Explanation:

The applicable regulatory factors are **State of Massachusetts Data Protection Act** and **State of Nevada Security of Personal Information Requirements**. HITRUST assessment scoping uses regulatory factors to tailor the requirement statements and implementation considerations applicable to an assessed organization's systems, data, and operating jurisdictions. Because the identified systems and applications serve customers in Massachusetts and Nevada, the corresponding state privacy and information-security obligations are relevant to the assessment scope.

Massachusetts' information-security regulations, commonly identified as 201 CMR 17.00, require persons that own or license personal information about Massachusetts residents to develop, implement, and maintain a comprehensive written information security program. This makes the Massachusetts regulatory factor applicable when the scoped environment handles those residents' personal information. See the Massachusetts 201 CMR 17.00 regulations.

Nevada's security and privacy provisions similarly apply to covered personal information associated with Nevada residents and establish obligations for safeguarding that information. Therefore, the Nevada regulatory factor is also appropriate for the assessment. The governing statutory provisions are available through the Nevada Revised Statutes, Chapter 603A.

QUESTION NO: 14

A pharmacy that accepts Medicare/Medicaid and also takes credit cards should include which regulatory factors in their assessment?

A. FISMA

B. FTC Red Flags Rule

C. PCI-DSS

D. FedRAMP

E. CMS (Centers for Medicare and Medicaid Services) Minimum Security Requirements (High)

ANSWER: B C E

Explanation:

FTC Red Flags Rule, PCI-DSS, and CMS (Centers for Medicare and Medicaid Services) Minimum Security Requirements (High) are the applicable regulatory factors to identify during assessment scoping. A pharmacy may maintain covered consumer accounts or otherwise act as a creditor, making identity-theft red-flag controls relevant to its account-opening and account-maintenance activities. The FTC's guidance describes the need for covered entities to maintain a written program that identifies, detects, responds to, and updates controls for identity-theft red flags.

Because the pharmacy accepts payment cards, its cardholder-data environment must be considered against PCI-DSS. PCI DSS establishes the baseline technical and operational safeguards for protecting account data throughout payment acceptance, transmission, storage, and supporting systems. See the PCI Security Standards Council's PCI DSS overview.

Participation in Medicare/Medicaid can also involve CMS information, systems, and security obligations. CMS Minimum Security Requirements (High) should therefore be included as a scoping factor when the pharmacy's services or information exchanges fall within CMS security requirements. CMS's security and privacy program describes its protection of information and systems at CMS Information Security and Privacy Program. Together, these factors capture identity-theft, payment-card, and CMS-related security obligations relevant to the pharmacy's operations.

QUESTION NO: 15

When generating a test plan the assessor must only use the Illustrative Procedures provided within the tool. [0054]

A. True

B. False

ANSWER: B

Explanation:

False is correct because HITRUST Illustrative Procedures are intended to help an assessor plan and perform testing, rather than to impose an exclusive set of testing steps. A test plan must be sufficient to evaluate whether the in-scope requirement and its associated control implementation are operating effectively in the assessed environment. This requires the assessor to apply professional judgment, consider the entity's unique systems, processes, risk factors, scope, and evidence available, and select procedures that generate appropriate and reliable evidence. The procedures presented in the assessment tool provide examples and a useful baseline, but an assessor may tailor them or use additional procedures when doing so is necessary to validate the requirement adequately. For example, the assessor may need to expand interviews, inspect additional configurations or records, increase sampling, or perform alternative validation procedures based on the implementation being assessed. This flexibility supports an assessment that is both risk-based and appropriately rigorous while remaining aligned to HITRUST assurance expectations. HITRUST describes the CSF as a framework supporting scalable, tailored assurance, as reflected in its HITRUST CSF overview and assurance-services information.

QUESTION NO: 16

On an r2 assessment, the decision to require a CAP for a deficiency (gap) is determined at the Control Reference level and the Requirement Statement level.

A. True

B. False

ANSWER: B

Explanation:

False is correct. In an HITRUST r2 assessment, a corrective action plan (CAP) requirement is determined at the Control Reference level. The Control Reference is the assessment-level object used to evaluate the implementation and effectiveness of the applicable control requirement and to determine whether an identified deficiency requires formal remediation through a CAP. Requirement Statements provide the detailed, testable implementation criteria within that Control Reference and are used to document assessment procedures, evidence, and specific gaps. They support the assessor's evaluation, but they do not create a separate, parallel CAP determination level. This distinction ensures that remediation is managed consistently for the assessed control while retaining traceability to the underlying requirement-level observations and evidence. HITRUST's r2 assessment approach is designed to provide a consistent and risk-based evaluation of the organization's implementation of the HITRUST CSF, including the handling of identified deficiencies and remediation activities. See HITRUST's overview of the HITRUST r2 Validated Assessment and its HITRUST CSF resources.