HITRUST

HITRUST CSF® Assurance Program Requirements

October 2019

Contents

Introduction & Purpose

The purpose of this document is to define the requirements for those organizations assessing their security and privacy program against the HITRUST CSF or attempting to obtain HITRUST CSF security certification. HITRUST External Assessors and those organizations seeking the HITRUST External Assessor designation should also refer to this document to ensure adequate understanding of the CSF Assurance Program and related processes.

This document is focused on addressing the process for an organization to assess its internal security and/or privacy programs against the requirements of the HITRUST CSF. The following documents located in the downloads section of the HITRUST website should be referenced for program background and familiarity with the HITRUST CSF and the HITRUST CSF Assurance Program:

- HITRUST CSF License Agreement
- HITRUST RMF Whitepaper
- Risk Analysis Guide for HITRUST Organizations and Assessors
- HITRUST CSF Assessment Methodology
- HITRUST External Assessor Requirements
- Evaluating Control Maturity using the HITRUST Approach
- HITRUST CSF Control Maturity Scoring Rubric

Background

The HITRUST CSF Assurance Program utilizes a common set of information security and privacy requirements with standardized assessment and reporting processes accepted and adopted by organizations and assessors. Through the HITRUST CSF Assurance Program, organizations and business partners can improve efficiencies and reduce the number and costs of security and privacy assessments.

The HITRUST CSF Assurance Program provides a practical mechanism for validating an organization's compliance with the HITRUST CSF, an overarching security and privacy framework that incorporates and leverages the existing security and privacy requirements, including federal and international legislation (e.g., HIPAA, GDPR), regulatory agency rules and guidance (e.g., NIST, FTC, CMS), state legislation (e.g., Nevada, Massachusetts, Texas), and industry frameworks (e.g., PCI, COBIT).

The standard requirements, methodology, and tools developed and maintained by HITRUST, in collaboration with information security and privacy professionals, enable both relying and assessed entities to implement a consistent approach to third-party compliance management. For the purposes of this document, "relying" and "assessed" will be used as general descriptors, and an "assessed organization" is any organization that undergoes a HITRUST CSF

assessment. A "relying party" is any party that accepts a HITRUST CSF Assessment report as an attestation of an assessed organization's control posture.

Under the HITRUST CSF Assurance Program, organizations can proactively or reactively, per a request from a relying entity, perform an assessment against the requirements of the HITRUST CSF. This single assessment will give an organization insight into its state of compliance against the various requirements incorporated into the CSF and can be used in lieu of proprietary requirements and processes for validating third-party compliance.

This program allows for an organization to receive immediate and incremental value from the CSF as it follows a logical path to certification. Unlike other programs, the oversight, vetting, and governance provided by HITRUST means greater industry-wide assurances and security.

Roles and Responsibilities

The following section describes the roles and responsibilities of each organization in the assessment process, including HITRUST, participating organizations, and approved HITRUST External Assessors. Each organization has specific roles with accompanying responsibilities that must be executed for an assessment to be validated or certified by HITRUST.

HITRUST Alliance, Inc.

HITRUST Alliance, Inc. serves as the governing organization of the HITRUST CSF. HITRUST Alliance, Inc.'s responsibilities include:

- Maintaining and updating the HITRUST CSF based on feedback from HITRUST External Assessors and participating organizations; and
- Supporting HITRUST External Assessors and participating organizations in interpreting HITRUST CSF control objectives, specifications, requirements, assessment procedures, risk factors, and standards/regulations cross-references.

HITRUST Services Corporation

HITRUST Services Corp ("HITRUST") provides the guidance, oversight, validation, and certification for the CSF Assurance Program. HITRUST's responsibilities in the assessment validation and certification process include:

- Approving assessor organizations and accrediting and training organizations and individuals who perform CSF assessments and/or assist participating organizations in implementing the HITRUST CSF;
- Sharing knowledge of security threats/vulnerabilities as well as successful mitigation strategies as provided by HITRUST External Assessors and participating organizations;
- Developing and providing approved assessment methodologies and tools for HITRUST External Assessors and participating organizations; and

- Issuing final validation or certification reports based on the HITRUST External Assessors' findings, and identification of required corrective actions as appropriate.

Participating Organizations

HITRUST participating organizations are those organizations that have adopted the HITRUST CSF as their security, privacy, and compliance framework for use internally and/or by third parties. Under the HITRUST CSF Assurance Program, a HITRUST participating organization's responsibilities include:

- Coordinating the performance of assessments and implementing corrective actions and organizational transformations as necessary;
- Funding its HITRUST CSF Assurance Program work, including assessments for validation and/or certification and corrective actions, performed by internal and external resources where required;
- Maintaining the information security management program that has been validated or certified through continuous monitoring, continuous review, and periodic reassessments; and
- Communicating actual or suspected data breaches involving the assessed environment to HITRUST.

Additionally, all organizations must have a mechanism to report to regulatory agencies; a HITRUST CSF Assessment Report is one way for organizations to meet such requirements.

Qualified Resources

HITRUST requires partner organizations and the individuals of partner/participating organizations to meet certain thresholds before receiving approval to perform HITRUST CSF-related work, including assessments, certifications, and remediation.

HITRUST defines four classifications of qualified resources:

- **Authorized External Assessor Organization** is a designation reserved for professional services firms or business units with the core business function of providing security, risk, and consulting services to other organizations.
- **Authorized Internal Assessor Function** is a designation reserved for departments or business units within assessed entities who perform HITRUST CSF assessment procedures.
- **HITRUST Certified CSF Practitioner (CCSFP)** is a designation reserved for individuals who have completed the CCSFP training course, passed the certification exam, and meet the required background and experience requirements necessary to effectively use the CSF. Such individuals typically work for a HITRUST External Assessor organization, a CSF user organization, or a firm/practice that provides HITRUST CSF consulting services.
- **Certified HITRUST Quality Professional (CHQP)** is a designation reserved for Certified CSF

Practitioners who act in a quality assurance role on CSF assessment engagements, have completed the CHQP training course, and have passed the CHQP certification exam. Such individuals typically work for a HITRUST External Assessor organization.

HITRUST also defines three specific roles within an external assessor's team, all of which are subject matter experts in the field of information security and/or privacy and are holders of HITRUST-issued certifications:

- The **Engagement Executive** is the CCSFP who owns the relationship between the External Assessor firm and the assessed entity. This individual is expected to review and approve the engagement scope, the test plan, testing results, and testing documentation.

- The **Engagement Lead** is the CCSFP responsible for the creation and execution of the test plan, performing/ overseeing sampling, analyzing test results, leading walkthroughs and interviews, and coordinating the validated assessment's day-to-day fieldwork.

- The **Quality Assurance Reviewer** is a CHQP who ensures that engagement execution meets internally defined and HITRUST-defined quality assurance requirements, including adequacy and completeness of the working papers, appropriate treatment of exceptions, and proper definition and application of scoping decisions.

Details on the specific requirements and process of becoming a qualified resource can be found in section 3 of the *HITRUST External Assessor Requirements* document.

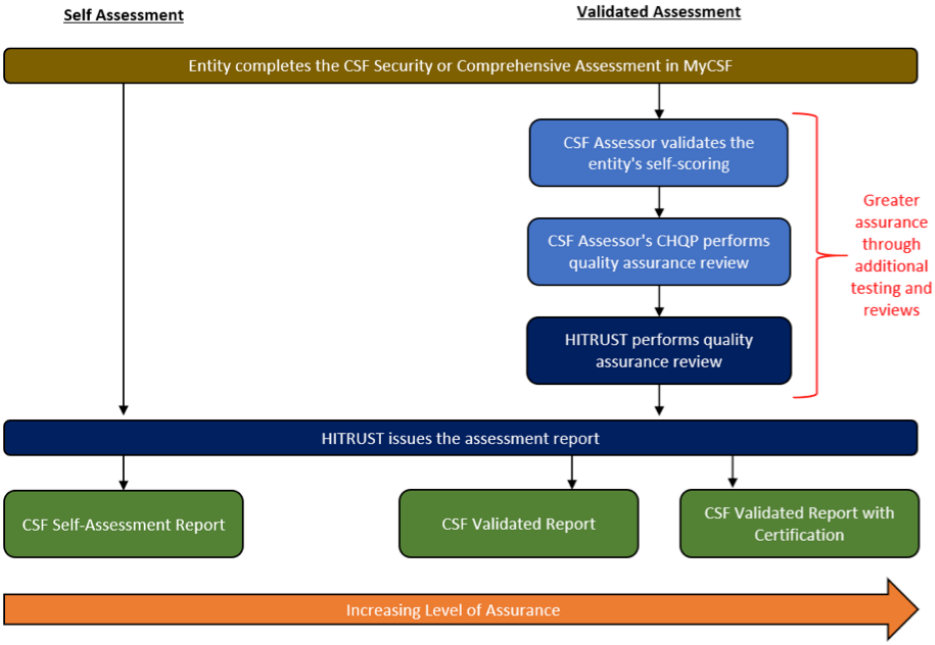
CSF Assurance Program Overview

The HITRUST CSF Assurance Program enables trust in information protection through an efficient and manageable approach by identifying incremental steps for an organization to take on the path to becoming HITRUST CSF Validated or HITRUST CSF Certified.

The comprehensiveness of the security and privacy requirements for the assessed entity is based on the multiple levels within the HITRUST CSF as determined by defined risk factors. The level of assurance for the overall assessment of the entity is based on multiple tiers, from self-assessments to validation by on-site testing performed by an Authorized External Assessor Organization. The results of the assessment are documented in a standard report with remediation activities tracked in corrective action plans (CAPs). Once vetted by HITRUST, the assessed entity can use the assessment results to report to external parties in lieu of existing security or privacy reporting processes, saving time and containing costs.

The diagram below outlines the relationship between comprehensiveness of the assessment and the level of assurance provided by the assessment for organizations of varying complexity based on the risk of the relationship as determined

by the relying organization:



A HITRUST CSF assessment allows an organization to communicate to relying entities its compliance with the HITRUST CSF and the NIST Cybersecurity Framework, and optionally with other requirements such as GDPR, PCI, MARS-E, and many others. HITRUST reviews the assessment results and CAPs to provide added assurance to the external entities relying on the assessed entity's results.

The HITRUST CSF Assurance Program effectively establishes trust in information protection through an achievable assessment and reporting path for organizations of all sizes, complexities, and risks. The HITRUST CSF Assurance Program operates at two levels: self-assessment and validated assessment. Certification is awarded to organizations that complete a validated assessment and meet the requisite scoring threshold and other certification criteria. The sections below describe general considerations when performing a self or a validated assessment. Please refer to the *HITRUST CSF Assessment Methodology* for more detailed guidance.

CSF Assessments

A HITRUST CSF assessment provides organizations with a means to assess and communicate their current state of security and compliance with external entities along with CAPs to address any identified gaps. An organization can, using the services of an Authorized External Assessor or by performing a self-assessment, conduct an assessment against the HITRUST CSF and have the results reported by HITRUST under the HITRUST CSF Assurance Program. The assessed entity is not required by HITRUST to meet all the security and privacy control requirements contained within the HITRUST CSF. Instead, HITRUST CSF assessments provide the assessed entity and the relying entity with a snapshot into the current state of security, privacy, and compliance of the assessed entity.

The level of assurance the assessed entity, and/or the relying entity on behalf of the assessed entity, has chosen determines the assessment strategy: self-assessment or validated assessment. As suggested by the name, a validated assessment provides a higher level of assurance since it includes independent and on-site third-party testing of controls, providing a more complete picture of security, privacy, and compliance to both the assessed entity and the relying entity.

Scope

Assessment scoping is the process of identifying the specific organizational business units, physical locations, systems, and other elements to be included in the CSF assessment. The scope will depend on the resources, security and privacy program maturity, and risk tolerance of an organization.

For organizations with standard operating procedures deployed consistently across the enterprise, HITRUST recommends selecting representative samples of assets for review versus testing every asset. For example, if the organization uses a standard operating system configuration, the external assessor would only need to review a statistically relevant sample. However, in organizations where security or privacy control consistency is lacking, the HITRUST participating organization and HITRUST External Assessor may determine that a review of all in-scope assets is required for certification.

Organizations undergoing a CSF validated assessment are required to prepare a verbose description of the system(s) and process(es) included in the assessment. This scope description should be written with as much detail about the system(s) and process(es) as possible and include descriptions of the service offering(s) and/or product(s) they support. Items to include in the scope description include component parts, internal vs. external development, connectivity, interfaces, and a high-level network or architecture diagram. It should also communicate if the environment as assessed as a whole, or, if partially assessed, what exclusions existed. This scope description should include a scope overview designed to communicate the assessment's scoping elements in summary form. HITRUST encourages the use of plain English and not industry insider-only language when describing the scope of an assessment; if uncommon acronyms must be used, they should be spelled out. While defining assessment scope is the responsibility of the assessed entity, the formal description of scope that is submitted to HITRUST for inclusion in the final assessment report should be jointly prepared through collaboration between the assessor and the assessed entity.

Additional resources to reference when scoping the assessment include the *HITRUST CSF Assessment Methodology* document.

Self-Assessments

Organizations may choose to self-assess using the standard methodology, requirements, and tools provided under the HITRUST CSF Assurance Program. Neither HITRUST nor a third-party performs any validation on the results of the self-assessment.

Using HITRUST's MyCSF tool, the organization being assessed first completes a risk-based scoping questionnaire that drives control selection and assessment scope based on general, organizational, geographical, systematic, and regulatory risk factors. Upon completion of the scoping questionnaire, a customized set of HITRUST CSF control references and requirement statements is generated in the MyCSF tool. The organization then enters responses for each

requirement statement and determines the level of compliance for each of the following five PRISMA-based maturity levels:

- Is a **policy** or standard in place?
- Is there a **process or procedure** to support the policy?
- Has it been **implemented**?
- It is being **measured** and tested by management to ensure it is operating?
- Are the **measured** results being managed to ensure corrective actions are taken as needed?

For each maturity level, the organization indicates its level of compliance. The five options are:

- Non-compliant (0%);
- Somewhat compliant (25%);
- Partially compliant (50%);
- Mostly compliant (75%); and
- Fully compliant (100%).

Once the organization has determined and entered compliance scores for each PRISMA maturity level across all requirement statements, it submits the populated MyCSF object to HITRUST for report generation.

HITRUST CSF Validated Assessments

HITRUST CSF validated assessments can be leveraged by organizations of any size or complexity and consist of more rigorous on-site testing performed by an Authorized External Assessor. The decision to undergo an on-site HITRUST CSF validated assessment should be based on the risk of the relationship between the assessed entity and the relying entity. For example, where two parties share a large amount of sensitive information, and/or the connectivity and access is high in relation to the number of systems and the risk of those systems, an on-site HITRUST CSF validated assessment may be necessary to provide a higher level of assurance to both parties. In cases where the HITRUST CSF validated assessment determines that the assessed entity meets all the security and/or privacy control requirements for HITRUST CSF certification, it will receive a validated assessment report with certification.

A validated assessment also utilizes HITRUST's MyCSF tool. As was the case for a self-assessment, the entity being assessed would begin by completing the risk-based scoping questionnaire in the MyCSF tool. Upon completion of the scoping questionnaire, a comprehensive and customized set of HITRUST CSF control references and requirement statements will be generated. The entity being assessed responds to the requirement statements based upon the PRISMA maturity model, ensuring that they are answered accurately. Once the organization has determined and entered compliance scores for each PRISMA maturity level across all requirement statements, it submits the populated MyCSF object to its external assessor for validation.

Validation Procedures

External Assessors are required to perform a sufficient level of on-site walkthroughs and testing of control documentation to: (i) confirm/validate the assessed entity's self-identified scoring levels/responses, and (ii) to ensure that compliance gaps have been appropriately identified. CSF requirement statements that are required for HITRUST CSF certification must be validated and are done so through a variety of testing strategies. This is to provide assurance to those relying entities that the control is in fact implemented and operating effectively. Procedures performed by assessors during validated assessment fieldwork include:

- On-site walkthroughs with and interviews of personnel to verify that policies and procedures are documented and implemented;
- Inspection of written CSF-relevant policies and procedures to ensure sufficient coverage of CSF requirements;
- Observation of the performance or existence of relevant controls and control processes;
- Inspection of documentation evidencing the existence/performance of relevant controls, including inspection of documentation associated with samples;
- Performance of technical testing to validate the implementation or operation of relevant controls;
- Inspection of operational or independent measures or metrics used by the organization; and
- Inspection of evidence generated by mechanisms used by the organization to manage relevant controls.

These testing strategies are consistent with the guidance provided by the National Institute of Standards and Technology (NIST) as outlined in their Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*. Although the most appropriate testing strategy and the extent of testing can be a matter of judgment, HITRUST External Assessors must ensure that both are consistent with the guidance provided by HITRUST and the illustrative procedures included in MyCSF.

All testing performed by the HITRUST External Assessor in support of the validated assessment must be conducted within 90 days of the submission date to HITRUST. All control processes, system configurations, implemented tools, written policies, and written procedures should be in operation/established for at least 90 days in order to be considered by the assessor during the validated assessment effort. Reliance on testing beyond this 90-day threshold, on controls in operation less than 90 days, or on written policies and procedures in existence for less than 90 days requires HITRUST approval prior to submission.

External assessors are expected to hold interviews and walkthroughs directly with control owners (and not through a proxy, such as an Internal Auditor, consultant, or Compliance Analyst).

Additional guidance on conducting a validated assessment and testing can be found in the HITRUST CSF Assessment Methodology document.

Test Plan

During the planning phase of a validated assessment effort, the HITRUST External Assessor must prepare a test plan which outlines the anticipated testing of all applicable/in-scope requirement statements; it serves as the blueprint for the performance of the validated assessment. The test plan shouldn't be a straight copy and paste repeat of the illustrative procedures defined by HITRUST. While helpful, these haven't been tailored enough to the match the specifics of the client's environment or to be quickly followed by team members in the field. Instead, the test plan should be based on the HITRUST-provided illustrative procedures associated with each PRISMA maturity level of each applicable/in-scope CSF requirement statement. The test plan should also include details on any sampling that is used for testing (e.g., how the sample will be selected, population source, etc.). Test plans should also identify who in the authorized external assessor organization will act as the Engagement Executive, QA Reviewer, and Engagement Lead and should be signed-off by the Engagement Executive, Engagement Lead, and optionally by the QA Reviewer before fieldwork commences. The test plan is not complete unless test steps have been drafted for all PRISMA levels across all in-scope requirement statements. Unless certain PRISMA levels for specific requirement statements have been specifically excluded from the scope of testing, each PRISMA level needs a test procedure prepared (in such case, a scoping note to that effect should be included in the test plan).

Areas that need to be understood by the External Assessor prior to developing a test plan include:

- the systems, business processes, and physical locations to be assessed;
- the risk factors to be assessed against;
- the nature of populations from which samples will be pulled (e.g., users, endpoints, network devices, mobile devices); and
- any CSF requirement statements which may have a shared responsibility.

Working Papers

Assessors must create working papers from artifacts collected during the validated assessment which were used to support the assessor's agreement with the assessed entity's scoring/responses. Each working paper must include the following markup:

- the name of the assessment;
- the name of the person that tested the working paper;
- the date the working paper was tested;
- a description of the associated test procedure;
- the result of the associated test procedure;
- (optional best practice) the date the evidence/artifact was created or pulled from the source system (e.g., in the form of a date stamp clearly visible in the log, report, screenshot, etc. being examined);
- (optional best practice) a clear identification of the associated scoping elements (e.g., systems, facilities, business units) being tested in that working paper.

These working paper markup elements are not specifically required for written policies and procedure workpapers. However, including markup in these documents can help them stand on their own and can benefit reviewers, the client, and subsequent assessor teams.

Note that a validated assessment's collective body of working papers is considered incomplete if validation of only a portion of an assessment's scope is reflected in the working papers. For example, working papers which include screenshots from only one of the two in-scope applications' configurations would be rejected during HITRUST's quality assurance checks.

All working papers created by an assessor in the course of a validated assessment must be attached to or referenced within MyCSF†. As documents are being attached or referenced, assessors are expected to consistently link each to the related requirement statement as well as the related PRISMA maturity level(s) (e.g., implemented). MyCSF features several edit checks associated with workpapers. For example, any requirement statements scored as mostly compliant or fully compliant in the policy and procedure levels must have documents linked to those levels.

Sampling

External Assessors are often required to perform sampling in order to validate management's self-scoring. HITRUST recommends establishing a standardized template for use in documenting the results of sampling-based test procedures. At a minimum, this standardized sampling template should capture the following sampling data points:

- population source (e.g., the organization's HR system);
- population size (e.g., 100 terminated employees);
- population date range (e.g., terminations occurring in calendar year 20XX);
- minimum required sample size per sampling requirements (e.g., 10 samples);
- sampling method (random, systematic, or haphazard); and
- procedures performed to ensure the completeness and accuracy of the population.

When performing sampling tests featuring homogeneous supporting evidence, assessor teams are not required to add the electronic markup to every sample item's markup. For the sake of efficiency, when supporting evidence is homogeneous, assessor teams need only to add the required electronic markup to one sample item's workpaper.

Additional information regarding the performance of sampling can be found in the HITRUST Assurance Methodology document.

Documenting Exceptions

Documenting exceptions noted by the External Assessor in the course of validated assessment fieldwork should be captured in MyCSF's "Assessor Comment" fields and/or within accompanying workpapers to enable reviewers—such as the External Assessor's QA Reviewer, the Engagement Lead, the Engagement Executive, and HITRUST's QA function—to easily reconcile to PRISMA maturity levels, corrective action plans, and working papers. Any conditions noted by the External Assessor necessitating a change in scoring should be discussed and agreed with management of the assessed

entity. Any exceptions noted by the assessor leading to scores of less than 100% (fully compliant) on the policy, procedure, or implemented PRISMA maturity levels should be formally document within the assessor's test results and should be described within MyCSF's "Assessor Comments" fields.

Pre-submission Quality Assurance Review

Prior to submitting a validated assessment to HITRUST for review and report assembly, the assessor's Engagement Executive as well as a Certified HITRUST Quality Professional (CHQP) within the assessor firm is required to perform a quality assurance review of the assessment's documentation. This pre-submission QA review should be driven by and documented through the HITRUST External Assessor Quality Checklist available for download within MyCSF as well as on the HITRUST website. This review generally focuses on whether the HITRUST CSF Assurance program requirements outlined in this document as well as in the HITRUST CSF Assurance Methodology document were observed. When performing his/her review, a CHQP's review considerations include areas such as:

- Have all required documents (listed in *Appendix B* of this document) been populated and attached into MyCSF?
- Where validation procedures outlined in the test plan reflective of the requirement statements' illustrative procedures. For example, was a sample selected if the illustrative procedure called for sampling?
- Where applicable, were sampling attributes clearly documented, including the basis for the selection of the population, the method of sample selection?
- Do facts presented in the client comments, assessor comments, and working papers support the scoring levels indicated by the entity and agreed upon by the assessor team?
- Is the timesheet in MyCSF reflective of the actual hours worked by the assessor team?
- Have all timing requirements, such as validated assessment procedures being performed within 90 days of submission date, been observed?

Submitting Results to HITRUST

Refer to *Appendix B* for the documents to be submitted to HITRUST following an on-site validated assessment.

Using the Work of Others

Recently completed audits and/or assessments covering some or all of the control areas included in the scope of a HITRUST validated assessment can possibly be leveraged (relied upon or inherited) by the external assessor. Reliance on the results of such efforts can benefit the assessed entity as well as the external assessor, as duplicative assessment-related requests and interviews can be minimized.

Nothing in this section requires the external assessor to utilize the work of others during a validated assessment.

The decision to rely on the work of others lies solely with the external assessor, as the external assessor is ultimately accountable for validating an assessed entity's implementation of the HITRUST CSF. When using the work of others, the external assessor should take care to design a validated assessment strategy that ensures they are still sufficiently involved in the validated assessment.

HITRUST recognizes three distinct approaches for an external assessor to utilize the work of others to reduce the extent of the external assessor's direct testing:

1. Inheritance of results of another validated HITRUST CSF assessment.
2. Reliance on audits and/or assessments performed by a third party.
3. Reliance on testing performed by the assessed entity (i.e., by internal assessors).

Inheritance of results of another validated HITRUST CSF assessment

The scoring conclusions documented in another validated HITRUST CSF assessment can be inherited to reduce the extent of the external assessor's direct testing. The following requirements must be met in order for inheritance from another validated HITRUST CSF assessment to occur (all of which are enforced by or enabled through MyCSF):

1. A valid business justification must exist for the inheritance. For example, it would be inappropriate to inherit from a service provider that does not actually provide services relevant to the scope of the assessed entity's validated assessment.
2. The other HITRUST CSF assessment must be completed with the final report posted in MyCSF.
3. The other HITRUST CSF assessment object must be configured to allow inheritance. The organization holding that HITRUST CSF certification must hold either a corporate or premier MyCSF subscription level in order for their assessment object to be inheritable.
4. The other HITRUST CSF certification must be less than two years old and the interim assessment must have been completed by the one-year certification anniversary.
5. The organization holding the HITRUST CSF assessment object being inherited from must approve the request(s) for inheritance which are initiated by its customer.

Reliance on audits and/or assessments performed by a third party

The results of recently completed audits performed by a third-party auditor against the scoped environment can—at the external assessor's discretion—be relied upon to reduce the extent of the external assessor's direct testing.

The following requirements must be met in order for reliance to be placed on the results of third-party audits:

1. A valid business justification must exist for relying on the third-party report. For example, it would be inappropriate to rely on a SOC 2 Type II report covering a service provider that is not actually used by the assessed entity.

2. A formal, final report documenting the results of the third-party audit must exist at the time of the start of the external assessor's fieldwork. *Third-party audits failing to produce a final report inclusive of the following elements should not be relied upon by the external assessor:*

    a) a description of the audit's scope;

    b) the timeframe that the testing covers (for period-of-time reports), the date that the final report was issued (for point-in-time reports), or the timeframe that the report is valid through (for forward-looking reports);

    c) the auditor's procedures performed;

    d) the conclusions reached for each control/requirement tested; and

    e) the compliance gaps / testing exceptions noted.

3. The third-party auditor must be independent of management and objective of the controls and processes audited. "Objectivity" refers to a lack of bias, judgment, or prejudice, and "independent" means not being influenced or controlled by others in matters of opinion, conduct, etc. *Only third-party audits performed by individuals sufficiently independent of the assessed entity and objective of the controls / requirements tested should be relied upon.*

4. *Third-party audits older than one year in age should not be relied upon.* This one-year reliance threshold is determined by comparing the start date of the external assessor's fieldwork to the following:

    a) For point-in-time reports (such as a PCI DSS ROC): To the date of the third-party auditor's final report.

    b) For period-of-time reports (such as a SOC 2 Type II report): To the end date of the reporting period.

    c) For future-looking certifications (such as an ISO 27001 certification): To the certification date or to the date of the most recent surveillance audit / interim assessment.

5. The external assessor and HITRUST must both be authorized recipients of the third-party audit report. While the external assessor and HITRUST don't need to be explicitly named as authorized recipients, the owner of the report must be allowed to distribute the report to such parties. This requirement exists specifically to avoid situations in which reliance was placed on a report that can't be shared with HITRUST, thus restricting HITRUST's ability to perform meaningful QA procedures. *Reliance cannot be placed on third-party audit reports for which neither HITRUST nor the external assessor are authorized to receive.*

6. The scope of the third-party audit (in terms of systems, facilities, and business units) must overlap with that of the HITRUST validated assessment. *Third-party audits of only systems or organizational elements outside the scope of the validated assessment should not be relied upon.*

7. The controls assessed in the third-party audit must overlap with that of the HITRUST validated assessment. *Third-party audits of only controls or compliance requirements outside the scope of the validated*

assessment should not be relied upon.

8. When designing a reliance strategy, the external assessor must map the HITRUST CSF requirement statements included in the HITRUST validated assessment (and related CSF elements included in the requirement statements' POLICY illustrative procedures) to the controls / requirements tested in the third-party audit. *In the absence of this mapping, the external assessor cannot form a meaningful reliance strategy and therefore lacks an adequate basis for reliance. To support HITRUST's QA efforts, this mapping as well as the third-party audit report must be attached to or referenced in MyCSF †.*

9. The depth / rigor of testing performed by the third-party auditor must reasonably align with the testing expectations placed upon external assessors by HITRUST. *Only those audits and assessments featuring tests of control design / operation / implementation / effectiveness through procedures such as inspection of evidentiary matter and sampling (utilizing statistically meaningful sample sizes as applicable) are suitable reliance.* For example, procedures executed by a service organization's auditor during a SOC 2 Type I examination should not be relied upon given a SOC 2 Type I examination's lack of substantive testing.

10. The third-party audit report must be prepared in accordance with the corresponding professional standards. *A third-party audit report that is not prepared in accordance with the corresponding professional standards should not be relied upon.*

When reliance is placed on a third-party audit report to reduce the extent of the external assessor's direct testing, the external assessor's workpaper documentation must indicate:

- The third-party audit report upon which reliance was placed.*
- The type or focus of the third-party audit (e.g., SOC 2 Type II).*
- The third-party audit's final report date.*
- The external assessor's mapping of the HITRUST CSF requirement statements included in the HITRUST validated assessment (and related CSF elements included in the requirement statements' POLICY illustrative procedures) to the controls / requirements tested in the third-party audit.

The external assessor's workpaper documentation must also contain a copy of the third-party audit report that was relied upon. This report must either be attached to or referenced within MyCSF†.

Reliance on testing performed by the assessed entity (i.e., by internal assessors)

In advance of a validated assessment, an assessed entity may perform assessment procedures against the HITRUST CSF internally, either using an organizational function (e.g., Internal Audit) or via an outside party (e.g., an authorized CSF assessor organization, a professional services firm possessing a HITRUST Readiness License). The individuals performing this testing are referred to as "Internal Assessors" and their function / team is referred to as the "Internal Assessor Function". The results of recently completed testing performed by internal assessors can—at

the external assessor's discretion—be relied upon by the external assessor to reduce the extent of the external assessor's direct testing.

Note that this guidance should not be interpreted as mandating that the assessed entity perform detailed testing in support of its self-scoring exercise included in all validated assessments; only external assessors are required to perform testing. However, if the assessed entity chooses to perform testing that can be leveraged by their external assessor, this guidance:

- Establishes a framework for the external assessor—at their discretion—to rely on that testing.
- Defines the requirements that must be met by both by the assessed entity and by the external assessor in order for such reliance to occur.
- Sets forth requirements which prevent over-reliance and undue reliance on an internal assessor's testing.

Regardless of the amount of reliance placed upon the work of an internal assessor function, the external assessor must lead and/or participate in on-site walkthroughs of the assessed entity's control environment. A "walkthrough" is the combination of inquiry of control owners with either observation or inspection of supporting evidence to corroborate the points discussed. For example: A walkthrough of a password expiration control might involve asking a system administrator to describe how and if the system enforces password expiration paired with observing the system's password expiration configuration during the discussion. As another example: Walking through an organization's security incident handling process might involve asking the process owner to describe the steps of the process while inspecting the documentation produced as a result of a recent security incident. In the context of reliance on the work of an internal assessor, walkthroughs allow the external assessor the insights necessary to evaluate the adequacy of the design of the internal assessor's tests. For example, through walkthroughs the external assessor may learn that two separate anti-malware solutions are in use (one for workstations and another for servers); if the internal assessor only tested one anti-malware solution, the design of the internal assessor's testing would be deemed deficient.

The following requirements **must be met** in order for an external assessor to place reliance on an internal assessor's testing:

1) *Testing performed on behalf of management by an outside party lacking a license to use the HITRUST CSF in a commercial context should not be relied upon by the external assessor.* If an outside party performed or was engaged to act as an internal assessor (i.e., through a "facilitated self-assessment"), that outside party must be either:

    a) A professional services firm designated as an Authorized External Assessor Organization (previously referred to as an "Approved HITRUST CSF Assessor"),

    b) In possession of a HITRUST Readiness License specific to the engagement, or

    c) An agent of management (e.g. through a loan staff, staff augmentation, or contractor arrangement.)

2) The internal assessor function must be approved by HITRUST through an application process. See *https://hitrustalliance.net/internal-assessors/* for more information. *Testing performed by an organizational function not previously authorized by HITRUST should not be relied upon by the external assessor.*

3) The internal assessor's testing conclusions (i.e., per-CSF requirement, per-PRISMA level scoring) must be entered into MyCSF. Also, accompanying workpapers must be attached to or referenced in MyCSF†.

4) *The internal assessor function must be objective of the controls and processes being tested.* "Objectivity" refers to a lack of bias, judgment, or prejudice. Example situations where objectivity is not considered to exist include:

    a) When the internal assessor function and the function being assessed (e.g., IT) roll up to the same executive.

    b) When the internal assessors are involved in the design, implementation, or operation of the controls being tested.

5) The internal assessor must be competent with respect to the HITRUST CSF, the HITRUST CSF Assurance Program Requirements, and the overall HITRUST validated assessment process. "Competence" is the set of demonstrable characteristics and skills that enable, and improve the efficiency of, performance of a job. *Testing performed by individuals lacking the necessary competence should not be relied upon by the external assessor.*

6) All internal assessors must hold an active CCSFP credential in order for testing to be relied upon by the external assessor (i.e., 100% of hours incurred by the internal assessor function must be incurred by a CCSFP). *Where this 100% hours threshold is not met, the external assessor should not rely on the internal assessor function's testing.*

7) The internal assessor's testing cannot be based on evidence more than 90 days old. *Internal assessor testing using evidence greater than 90 days old should not be relied upon by the external assessor.* This 90-day age threshold is determined by comparing external assessor's validated assessment fieldwork start date to:

    a) The date the associated evidence was produced / generated / captured (for point-in-time evidence such as screenshots of configurations),

    b) The end date of the population date range (for period-of-time populations such as the listing of newly hired employees), or

    c) The date of the observation (for observation-based tests).

8) The scope of the internal assessor's testing (in terms of systems, facilities, and business units) must mirror that of the HITRUST validated assessment. *An internal assessor's testing of out-of-scope systems, facilities*

and organizational elements should not be relied upon by the external assessor.

9) The depth / rigor of testing performed by the internal assessor must adhere to the HITRUST's testing expectations placed upon external assessors. Specifically, the internal assessor's testing must be performed in accordance with requirements set forth in this document and in the *CSF Assessment Methodology*. *Internal assessor testing which fails to adhere to HITRUST's assessment requirements should not be relied upon by the external assessor.*

10) The testing documentation and supporting workpapers produced by the internal assessor must adhere to HITRUST's assessment documentation requirements placed upon external assessors. Specifically, the internal assessor's testing must be documented in accordance with requirements set forth in the *HITRUST CSF Assurance Program Documentation Requirements*. *Poorly documented testing performed by internal assessors should not be relied upon by the external assessor.*

11) To gain comfort that the internal assessor's tests were adequately executed, the external assessor (i) must be provided the internal assessor's workpapers and (ii) must reperform (through inspection of those workpapers) a portion of the internal assessor's testing. "Reperforming" an internal assessor's testing involves inspecting, in detail, the evidence examined by the internal assessor and reconciling the information therein to (a) the conclusions / scoring levels reached by the internal assessor, and (b) to information gleaned through the external assessor's walkthroughs of the control environment. The aim of reperforming an internal assessor's testing is to gain reasonable comfort that the internal assessor collected the same evidence, tested the same attributes, and reached the same conclusions that the external assessor would have had reliance not occurred. When placing reliance on an internal assessor's sample-based test, the external assessor is expected to perform the internal assessor's testing of 20% of the sample (rounding up to the nearest whole number as necessary); otherwise, the external assessor must reperform all aspects of the test. *If reperformance of the internal assessor's testing yields results that call into question the adequacy of the internal assessor's testing or accompanying documentation, the external assessor should either not place reliance on that testing, supplement the internal assessor's testing to address the identified testing gap(s), or allow the internal assessor the opportunity to remediate the testing gap.*

When reliance is placed on an internal assessor's testing to reduce the extent of the external assessor's direct testing, **the external assessor's documentation**, as captured in MyCSF, must clearly reflect / include:

- An identification of the HITRUST CSF requirement statements where reliance on the internal assessor's testing was placed.

- Confirmation that external assessor reperformed the internal assessor's testing and addressed identified testing flaws through either (a) not placing reliance on the flawed testing, (b) supplementing the testing to address the identified testing flaws, or (c) allowing the internal assessor the opportunity to remediate the flawed testing.

- For sample-based tests being relied upon, an identification of which and how many sample(s) were

reperformed by the external assessor along with the conclusions reached by the external assessor for each reperformed item.

When reliance is placed on an internal assessor's testing to reduce the extent of the external assessor's direct testing, **the internal assessor's documentation**, as captured in MyCSF, must clearly reflect / include:

- The scoring levels reached by the internal assessor on a per-CSF requirement, per-PRISMA level basis.
- A populated internal assessor timesheet reflective of the hours incurred by the internal assessor function.
- The internal assessor's workpapers / supporting evidence (either attached to or referenced)†.

HITRUST CSF Certified

"HITRUST CSF Certified" refers to an organization that has met all CSF certification requirements as defined by HITRUST based on industry input and analysis. "CSF Certification" involves performance of a validated assessment leveraging the MyCSF tool, the embedded HITRUST CSF control requirement statements, and the PRISMA maturity model. CSF certification provides relying entities with greater assurance that an assessed entity is appropriately managing risk. CSF certification is designed to remove the variability in acceptable security and privacy requirements by establishing a baseline defined by industry, removing unnecessary and costly negotiations and risk acceptance. In being HITRUST CSF Certified, an organization is communicating to its business partners and other third-party entities (e.g., regulatory agencies) that protection of sensitive information is both a necessity and priority, that essential security and privacy controls are in place, and that management is committed to information security and privacy.

Granting Certification

The decision for granting certification to an organization is based on the testing results of the HITRUST External Assessor and ultimately reviewed, approved, and certified by HITRUST. To be HITRUST CSF Certified, the organization must:

- Successfully demonstrate meeting all controls in the CSF required for the current year's certification at the appropriate level required for the organization based on its responses to the MyCSF requirement statements; and
- Achieve a rating of "3" or higher on HITRUST's scale of 1 to 5 for each of the 19 domains documented in MyCSF. (Note that under certain circumstances organizations may be HITRUST CSF Certified with a "3" rating in one or more domains. In these instances, the risk must be inherently low and corrective action plans must be documented in the report.)

Where certification is granted, certification is valid for 24 months from the certification date on the condition that the interim assessment and continuous monitoring requirements are met.

The development of the CSF and requirements for certification continually evolve to account for new regulatory

requirements, standards, environmental changes, technologies, and vulnerabilities. Because of this, certifications are designated by the CSF version to distinguish the CSF versions and certification requirements applicable. Please refer to *Appendix A* for a complete list of the current CSF controls required for certification.

HITRUST CSF Certifications contain the wording *"meets the HITRUST CSF vX Certification Criteria"*. The scope of certification is included on the Letter of Certification and further defined in the report to provide details on the organization's systems covered by the assessment. It is up to HITRUST's discretion as to whether multiple certificates are issued in circumstances where multiple systems are certified.

De-certification

Upon discovery or suspicion of a data security breach, the compromised entity must notify HITRUST. HITRUST CSF Certified entities that experience an actual or suspected data security breach will undergo an investigation initiated by HITRUST and at the entities' expense with an Approved HITRUST External Assessor organization of HITRUST's choosing to evaluate the nature of the breach. If the breach is deemed to be material to the entity's certification (for example, a control failure by the HITRUST CSF Certified organization for a required control, or a misrepresentation of a required control by either the HITRUST External Assessor or HITRUST CSF Certified organization), the certification will be suspended. Immaterial breaches not related to the required controls of the CSF will not result in suspension of the certification or de-certification.

For the HITRUST CSF Certified status to be reinstated by HITRUST, the compromised entity must perform an analysis of the breach, which shall include a forensics analysis if the breach resulted in whole or in part due to a failure of technical controls. The results of the analysis, accompanied by a detailed CAP specific to the incident, must be submitted to HITRUST for review. After successful completion of the plan, the compromised entity must bring in an Approved HITRUST External Assessor to review and assess the corrective actions and provide any findings to HITRUST. If no gaps are noted, the HITRUST CSF Certified status will be reinstated for the compromised entity.

For a two-year period following the breach, the compromised entity will be re-assessed annually following the original assessment process and include all HITRUST CSF controls.

Interim Assessment

For an entity to retain its certification for a two-year period, an interim assessment must be completed and submitted to HITRUST in the 90-day window leading up to the one-year anniversary of the certification issuance date. For MyCSF subscribers, the interim assessment is generated automatically 90 days prior to the required submission date. Customers can also manually generate the object 120 days prior. All interim assessments for objects using CSF version 9.1 or later are required to be performed in MyCSF.

The following steps outline what is expected of the External Assessor during an interim assessment:

- Ask the assessed entity to update the MyCSF object that was the basis for the initial assessment.
- Review the updated MyCSF object with management of the assessed entity and note any changes to the environment and control requirement responses.

- For each of the 19 assessment domains, discuss with the owner(s) any changes noted or verify that no changes had occurred.

- Where a significant change to a domain or control requirement has occurred, determine its impact, and test the new/updated control. For example, if the client implemented a new email encryption tool, test the new tool to ensure it is operating and the settings are appropriate.

- Perform full testing/validation procedures for 19 requirement statements (1 per domain) randomly selected by the MyCSF tool, working with the assessed entity to re-score these requirement statements in MyCSF if necessary, based on the results of the test procedures performed. These validation procedures documented in the MyCSF tool in the organization's Interim Assessment Object. Note that all assessor expectations related to timing of validation procedures, performance of validation procedures, and creation of working papers apply equally to validated assessments (although a test plan is not required).

- Review the status of CAPs that were included in the initial assessment report and conclude as to whether the entity is making satisfactory progress. This is also documented in the MyCSF tool in the organization's Interim Assessment Object.

- Within the MyCSF tool, document indicate whether there have been significant changes, whether adequate progress was made on the CAPs and a recommendation as to whether or not the assessed entity should retain its certification.

- Submit the Interim Assessment Object to HITRUST for its review. If HITRUST concludes that the assessed entity should retain its certification, it will issue a letter to the entity that indicates its certification is still valid. If HITRUST concludes that it no longer meets the requirements, a letter will be sent to the entity asking it to remove any references to its HITRUST certification from its literature and website.

The interim assessment will be submitted to HITRUST by the assessor. Upon receipt, HITRUST then performs the same level of quality assurance checks as performed on a validated assessment submission.

Any acquisition of one entity or by another entity must be communicated to the HITRUST External Assessor immediately so that the scope and significance can be evaluated and communicated to HITRUST. Should a re-assessment be necessary, HITRUST will designate the assessed entity's HITRUST CSF Certified status as pending until the results of the re-assessment confirm that the changed environment continues to meet the requirements set forth.

Re-assessments

The purpose of the re-assessment is to validate the assessed entity is continuing to comply with the controls of the required HITRUST CSF controls required for certification. HITRUST requires that assessed entities conduct a complete re-assessment every second year. Re-assessments could occur sooner pending evaluation of a data security breach or significant change in the organization's operating environment as determined by the HITRUST External Assessor's professional judgment. For example, a full re-assessment may be required annually for an organization that is expanding operations (naturally or through mergers and acquisitions) or changing its environment and systems extensively and rapidly. In no event shall the

interval between re-assessments exceed 24 months. The process for the re-assessment will follow the original assessment process specified under the HITRUST CSF Assurance Program.

Corrective Action Plans

The Corrective Action Plan prepared by the assessed entity describes the specific measures that are planned to correct compliance gaps identified during the assessment for validation or certification. HITRUST understands that most organizations have more vulnerabilities than they have resources to address. Organizations should prioritize corrective actions based on the security and/or privacy category of the information systems, the direct effect the vulnerability has on the overall security and privacy posture of the information systems, and the requirements for HITRUST CSF certification.

The CAP should include, at a minimum, a control gap identifier, a description of the compliance gap, CSF requirement statement mapping, remediation owner, scheduled completion date, planned corrective action(s), and status. The HITRUST External Assessor should review the CAP to evaluate the effectiveness of the remediation strategy and provide any recommendations to the assessed entity. CAPs are only required for validated reports with certification and must be submitted to HITRUST within 30 days of the organization receiving a copy of the draft report.

Continuous Monitoring

Once an assessed entity has had its assessment certified by HITRUST, the entity enters a critical post-assessment period called continuous monitoring. While assessment and re-assessments are important to measure the implementation of security and privacy controls and compliance status at a point in time, they are not sufficient to ensure ongoing compliance and effective security between assessments and reviews.

Assessed entities must implement a continuous monitoring program to determine if the controls implemented in accordance with the HITRUST CSF continue to remain effective over time given the dynamic threat environment and that any identified gaps are remediated in accordance with the CAP.

HITRUST recommends continuous monitoring programs include configuration management for all information systems, security, and privacy risk analysis for planned or actual changes to an operational environment or an information system, ongoing selective evaluation of security and privacy controls, and frequent interaction between information systems management and the security and privacy teams.

HITRUST requires that security and privacy documentation (e.g., policies, procedures) and the CAP are updated frequently to reflect changes to the environment, systems, and/or security and privacy posture of the organization.

Appendix A: HITRUST CSF v9.3 Certification Requirements

00.a Information Security Management Program	07.c Acceptable Use of Assets
01.b User Registration	08.b Physical Entry Controls
01.c Privilege Management	08.d Protecting against External and Environmental Threats
01.d User Password Management	08.j Equipment Maintenance
01.e Review of User Access Rights	08.l Secure Disposal or Re-Use of Equipment
01.h Clear Desk and Clear Screen Policy	09.b Change Management
01.j User Authentication for External Connections	09.c Segregation of Duties
01.l Remote Diagnostic and Configuration Port Protection	09.e Service Delivery
01.m Segregation in Networks	09.f Monitoring and Review of Third-Party Services
01.n Network Connection Control	09.j Controls Against Malicious Code
01.o Network Routing Control	09.k Controls Against Mobile Code
01.q User Identification and Authentication	09.l Back-up
01.t Session Timeout	09.m Network Controls
01.v Information Access Restriction	09.n Security of Network Services
01.w Sensitive System Isolation	09.o Management of Removable Media
01.x Mobile Computing and Communications	09.p Disposal of Media
01.y Teleworking	09.q Information Handling Procedures
02.a Roles and Responsibilities	09.s Information Exchange Policies and Procedures
02.d Management Responsibilities	09.v Electronic Messaging
02.e Information Security Awareness, Education, and Training	09.x Electronic Commerce Services
02.f Disciplinary Process	09.y On-line Transactions
02.i Removal of Access Rights	09.aa Audit Logging
03.b Performing Risk Assessments	09.ab Monitoring System Use
03.c Risk Mitigation	09.ad Administrator and Operator Logs
03.d Risk Evaluation	10.a Security Requirements Analysis and Specification
04.a Information Security Policy Document	10.b Input Data Validation
04.b Review of the Information Security Policy	10.f Policy on the Use of Cryptographic Controls
05.a Management Commitment to Information Security	10.h Control of Operational Software
05.h Independent Review of Information Security	10.k Change Control Procedures
05.i Identification of Risks Related to External Parties	10.l Outsourced Software Development
05.j Addressing Security When Dealing with Customers	10.m Control of Technical Vulnerabilities
05.k Addressing Security in Third-Party Agreements	11.a Reporting Information Security Events
06.c Protection of Organizational Records	11.c Responsibilities and Procedures
06.d Data Protection and Privacy of Covered Information	11.d Learning from Information Security Incidents
06.e Prevention of Misuse of Information Assets	12.b Business Continuity and Risk Assessment
06.g Compliance with Security Policies and Standards	12.c Developing and Implementing Continuity Plans Including Information Security
06.h Technical Compliance Checking	12.d Business Continuity Planning Framework
07.a Inventory of Assets	

Appendix B: CSF On-site Assessment Submission Documents

External Assessors are required to ensure that the following documentation has been completed/included within MyCSF for all validated assessment submissions:

- a completed MyCSF Assessment Object;
- a test plan;
- the "Organizational Overview and Scope" (template located in MyCSF);
- a "Management Representation Letter" from the assessed entity, a copy of which can be found in "Documents" section of each assessment in MyCSF;
- the "Participation Agreement" signed by the assessed entity, a copy of which can be found in "Documents" section of each assessment in MyCSF;
- a completed "HITRUST External Assessor Quality Checklist", signed and initialed by the assessor's Engagement Executive and QA Reviewer;
- a completed assessor timesheet within MyCSF; and
- all working papers. These working papers must meet the minimum working paper requirements documented in the CSF Assurance Program Documentation Requirements.

Endnotes

† "Attaching" a file in MyCSF refers to the act of uploading the file into the tool, and "referencing" a file in MyCSF refers to the act of identifying the file by name or title in MyCSF without actually uploading that file.

* As documented in the HITRUST CSF Validated Assessment Report and communicated to HITRUST using the Organizational Overview and Scope document.

HITRUST®
855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net