HITRUST

HITRUST CSF® Assurance Program Requirements

Version 9.1

February 2018

Contents

Introduction & Purpose . . . 3
External References . . . 3
Background . . . 3
Roles and Responsibilities . . . 4
- HITRUST Alliance, Inc. . . . 4
- HITRUST Services Corporation . . . 4
- Participating Organizations . . . 5
- Qualified Resources . . . 5

HITRUST CSF Assurance Program Overview . . . 6
- Scope . . . 7
- Testing Strategy . . . 7

HITRUST CSF Assessments . . . 8
- Self Assessment . . . 8
- HITRUST CSF Validated . . . 9
- Testing . . . 9
- Submitting Results to HITRUST . . . 10

HITRUST CSF Certified . . . 10
- Granting Certification . . . 10
- De-certification . . . 11
- Interim Review . . . 11
- Re-assessments . . . 12

Corrective Action Plan . . . 13
Continuous Monitoring . . . 13
Appendix A: HITRUST CSF Certification Requirements . . . 14
Appendix B: HITRUST CSF Onsite Assessment Submission Documents . . . 15

Introduction & Purpose

The purpose of this document is to define the requirements for those organizations conducting an assessment of their security and privacy program against the HITRUST CSF or attempting to obtain HITRUST CSF security certification against the HITRUST CSF from HITRUST under the HITRUST CSF Assurance Program. HITRUST CSF Assessors and those organizations seeking the HITRUST CSF Assessor designation should also refer to this document to ensure adequate understanding of the process and applicable requirements.

External References

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 HITRUST documents located on the HITRUST web site in the "Downloads" section should be referenced for program background and familiarity with the HITRUST CSF:

- HITRUST CSF License Agreement
- HITRUST RMF Whitepaper
- Risk Analysis Guide for HITRUST Organizations and Assessors
- HITRUST CSF Assessment Methodology
- HITRUST CSF Assessor Requirements

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. 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., ARRA, HIPAAand GDPR), regulatory agency rules and guidance (e.g., NIST, FTC and CMS), state legislation (e.g., Nevada, Massachusetts and Texas), and industry frameworks (e.g., PCI and 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 description "relying"and "assessed" will be used as general descriptors. 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 CSF Assessors. Each organization has specific roles with accompanying responsibilities that must be executed in order 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.
- Supporting HITRUST CSF 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 the 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 CSF Assessors and participating organizations.
- Developing and providing approved assessment methodologies and tools for HITRUST CSF Assessors and participating organizations.
- Issuing final validation or certification reports based on the HITRUST CSF 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 used internally and/or for 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 re-assessments.
- 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 two classifications of qualified resources: **HITRUST CSF Assessors** and **HITRUST Certified CSF Practitioners**.

Approved HITRUST CSF Assessors is a designation reserved for organizations with the core business function of providing security, risk, and consulting services to other organizations across industry.

HITRUST Certified CSF Practitioners (CCSFP) is a designation reserved for individuals who have completed the CCSFP training course, passed the exam and meet the required background and experience requirements in order to be able to effectively use the HITRUST CSF. Because CCSFPs can be individuals employed by any type of organization, use of the HITRUST CSF is not limited to performing internal/external assessments. The HITRUST CSF should also be used as a reference for developing, revising, or maintaining a comprehensive information protection and compliance program.

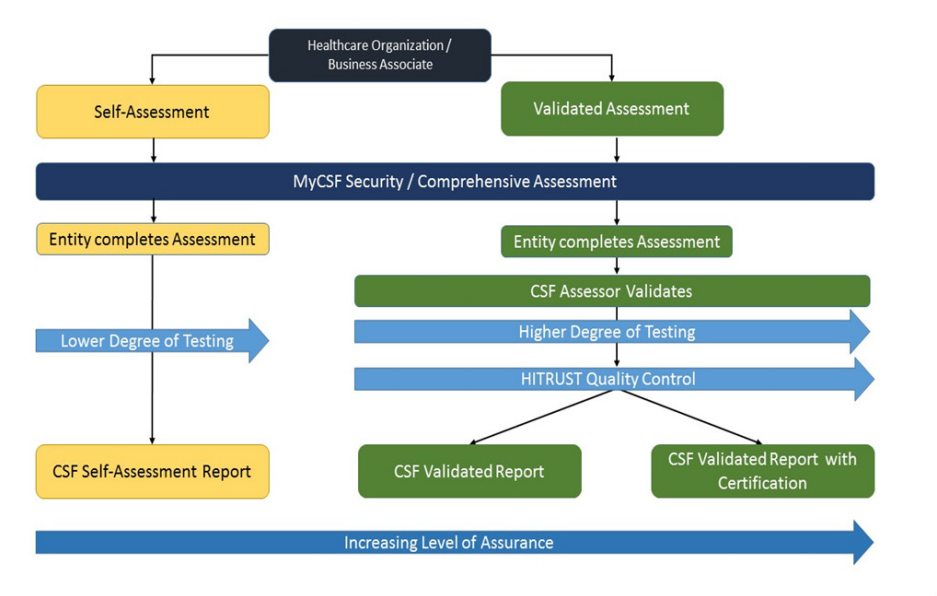
Details on the specific requirements and process of becoming a qualified resource can be found in section 3 of the *HITRUST CSF Assessor Requirements* document.

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 analysis/testing performed by an approved HITRUST CSF Assessor. The results of the assessment are documented in a standard report with remediation activities tracked in a corrective action plan (CAP). Once vetted by HITRUST and performed for all levels of assurance, the assessed entity can use the assessment results to report to external parties in lieu of existing security or privacy requirements and 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 optionally with other requirements such as GDPR, PCI, MARS-E, and NIST CsF. HITRUST reviews the assessment results and CAP 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.

Scope

Assessment scoping is the process for determining the scope of the assessment regarding organizational business units and related systems. This ensures that the necessary data is collected in an effective and efficient manner. The process is designed to be flexible and adaptive so that it can be tailored to fit the unique environment of an organization based on size and complexity.

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 CSF 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 CSF Assessor may determine that a review of all in-scope assets is required for certification.

By clearly defining and identifying upfront the scope of the CSF assessment at the organization, the assessor will focus and streamline analysis and information gathering tasks resulting in a timely completion of the assessment with a detailed report. Additional resources to reference when scoping the assessment include the *HITRUST CSF Assessment Methodology* document.

Testing Strategy

Controls that are required for HITRUST CSF certification must be validated 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. These strategies include examining documentation and processes, interviewing organization personnel, and testing system configurations. Sampling of systems during testing is permitted; sampling of organizational business units can be performed if the business units are similar and subject to the same policy requirements, but only for those controls addressed by the policies. If inconsistencies are noted in the sample, the assessor may make judgments about the variation and/or about the maturity rating based on the variation. Such judgments should be consistent with generally accepted sampling techniques and the maturity ratings fully justified before submitting an assessment for validation through MyCSF. Use of sampling, sample sizes and dealing with exceptions are covered in more detail in the *HITRUST CSF Assessment Methodology* document.

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 CSF Assessors must ensure that both are consistent with the guidance provided by HITRUST and the illustrative procedures included in MyCSF.

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 a HITRUST CSF Assessor or 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 third-party testing of controls, providing a more complete picture of security, privacy and compliance to both the assessed entity and the relying entity.

Self Assessment

Organizations may choose to self-assess using the standard methodology, requirements, and tools provided under the HITRUST CSF Assurance Program. HITRUST performs no validation on the results of the self-assessment.

Using HITRUST's MyCSF tool, the organization being assessed first completes a risk-based questionnaire that drives control selection and assessment scope based on organizational, regulatory and system profile information. Upon completion of the questionnaire, a customized set of HITRUST CSF control requirements statements will be generated that includes the required HITRUST CSF control specifications. The organization will enter responses for each requirements statement that will assess the level of compliance for each of five (5) PRISMA-based maturity levels. Those five maturity levels are as follows:

- 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
- Somewhat compliant
- Partially compliant
- Mostly compliant
- Fully compliant

Once the organization has responded to all the requirements statements, it submits the completed questionnaire to HITRUST for review and report generation.

HITRUST CSF Validated

HITRUST CSF Validated assessments are permitted for organizations of any size or complexity and consist of more rigorous on-site testing at the entity performed by an approved HITRUST CSF 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.

An on-site 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 questionnaire in the MyCSF tool. Upon completion of the questionnaire a comprehensive and customized set of requirements statements are generated. The entity being assessed responds to the requirements statements based upon the PRISMA maturity model described above for Self-Assessments and ensure that they are answered accurately in accordance with the requirements of the HITRUST CSF. Once completed with its responses, the assessed entity will submit the questionnaire to its Assessor for validation.

Testing

The HITRUST CSF Assessor will review any supporting documentation associated with the questions and CSF requirements to ensure it is sufficient to meet the security and privacy control requirements and that any missing documentation is gathered or noted as a gap. The HITRUST CSF Assessor will interview personnel of the assessed entity to verify that the policies and procedures documented are implemented at the required HITRUST CSF implementation level and are being followed. The results of the interviews and policy/procedure examinations will be used by the HITRUST CSF assessor to design and execute tests to validate the responses previously entered. Any previous/recent reviews or assessments can and should be used by the HITRUST CSF Assessor to assist in the review and testing process; however, any third-party reports that are relied upon in lieu of testing should be dated within 12 months of the submission date to HITRUST. Testing performed by the HITRUST CSF Assessor should have been conducted within 90 days of the submission date to HITRUST. Reliance on testing beyond this threshold requires HITRUST approval prior to submission. Additional guidance on conducting a validated assessment and testing can be found in the HITRUST CSF Assessment Methodology document.

Submitting Results to HITRUST

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

HITRUST CSF Certified

"HITRUST CSF Certified' refers to an organization that has met all of the certification requirements of the CSF 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 requirements statements and the PRISMA maturity model and 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. By being HITRUST CSF Certified, an organization is communicating to its business partners and other third-party entities (e.g., regulatory agencies) that sensitive information protection is both a necessity and priority, essential security and privacy controls are in place, and management is committed to information security and privacy.

Granting Certification

The decision for granting certification to an organization will be based on the testing results of the HITRUST CSF 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 requirements statements.
- Achieve a rating of 3+[1] or higher on HITRUST's scale of 1 to 5 for each control domain documented in MyCSF.

Where certification is granted, certification is valid for two years (24 months) from the certification date on the condition that the interim review and continuous monitoring requirements are met.

The development of the HITRUST CSF and requirements for certification are expected to evolve to account for new regulatory requirements, standards, environmental changes, technologies and vulnerabilities. Because of this, certification will be designated by the year and version number to distinguish the CSF versions and certification requirements applicable. Please refer to Appendix A for a complete list of the current CSF control specifications required for certification.

The HITRUST CSF Certified letter will contain the wording "*meets the HITRUST CSF vX Certification Criteria.* The scope of certification will be recorded on the certificate providing details on the organization's entities/business units and systems covered by the assessment. It is up to HITRUST's discretion as to whether multiple certificates will be issued in circumstances where multiple entities/business units are certified, or whether one certification report will be issued.

[1] *Under certain circumstances, organizations may be CSF Certified with a 3 rating in one or more domain areas documented in MyCSF. In these instances, the risk must be inherently low and a corrective action plan must be documented, budget approved, tasks in-progress, and the plan must be completed within a reasonable time from the date of certification.*

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 CSF Assessor organization of HITRUST's choosing to evaluate the nature of the breach. If it is material to the 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 CSF 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 CSF 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 Review

For an entity to retain its validation/certification for the two-year period as noted in the assessment report, an interim review must be completed after the first year. This review would normally be performed by the assessor who initially performed the validation/certification work. The review should be completed as close as possible to the one-year anniversary of the initial report date. HITRUST would expect to have evidence of the update having been performed within two months following the one-year anniversary date of the initial assessment report.

Although there is some flexibility on what procedures should be performed, the following steps outline what HITRUST would expect of the assessor:

- 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 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.
- Where no change has occurred for a given domain, select one or more of the key controls in that domain and perform appropriate testing of that control(s) to determine if it is still functioning.

- Review the status of CAPs that were included in the initial assessment report and conclude as to whether or not the entity is making satisfactory progress.
- Document the above procedures in a memo for HITRUST to review and include
  - Documents reviewed
  - Personnel interviewed
  - Tests performed and results
  - Progress related to the CAPs
  - Recommendation on entity retaining its certification

As appropriate, attach any supporting documentation to the memo.

Any acquisition of one entity or by another entity must be communicated to the HITRUST CSF 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.

Upon receipt of the memo from the assessor, HITRUST will review the findings and conclude as to whether or not the entity continues to meet the HITRUST CSF control requirements. If HITRUST concludes that it has, it will issue a letter (if requested) to the entity that indicates its validation/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 validation/certification from its literature and website.

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 CSF 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 Plan

The Corrective Action Plan (CAP) prepared by the assessed entity, and its assessor as applicable, describes the specific measures that are planned to correct deficiencies 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, control gap, HITRUST CSF control mapping, point of contact, scheduled completion date, corrective actions, and status. The HITRUST CSF Assessor must review the CAP to evaluate the effectiveness of the remediation strategy, provide recommendations, and document any findings for submission to HITRUST. 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. The assessment and re-assessments are important to measure the implementation of security and privacy controls and compliance status at a point in time, but it is not sufficient to ensure ongoing compliance and effective security between assessments and reviews.

Assessed entities need to 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.

The security and privacy teams and information system owner(s) should report progress made during the remediation process and are encouraged to report to HITRUST any innovative or successful measures taken when remediating gaps.

Appendix A: HITRUST CSF v9.1 Certification Requirements

Required for HITRUST Certification CSF v9.1	
0.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 Onsite Assessment Submission Documents

The following documentation is required to be submitted by the HITRUST CSF Assessor to HITRUST for Validated assessments:

- A completed MyCSF Assessment Object.
- A work plan including, as applicable, documentation reviewed, interviews conducted (name and role), technical configuration testing performed and results, and any prior assessments/reviews leveraged.
- A summary of assessment duration if not obvious from the work plan.
- Acknowledgement that all actions were performed in accordance with HITRUST policies, procedures, and applicable requirements, listing those individuals who performed the assessment and their roles in the engagement.
- A summary of the assessed entity's security management program including structure, governance, and key controls implemented if not included in MyCSF.
- The Organizational Overview and Scope found in the "Getting Started" tab in MyCSF.
- A "Third-Party Rep Letter" from the assessed entity, a copy of which can be found in the "Getting Started" tab in MyCSF.
- The "Third-Party Participation Agreement" signed by the assessed entity, a copy of which can be found in the "Getting Started" tab in MyCSF.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net