HITRUST

CSF Assurance Program Requirements

Version 1.3.1
Table of Contents

1 Introduction .......................................................................................................................................... 4
  1.1 Purpose ......................................................................................................................................... 4
  1.2 External References ...................................................................................................................... 4
  1.3 Background ................................................................................................................................... 4
  1.4 Roles and Responsibilities............................................................................................................. 5
    1.4.1 HITRUST Alliance, Inc. ........................................................................................................... 5
    1.4.2 HITRUST Services Corporation .............................................................................................. 5
    1.4.3 Member Organizations ......................................................................................................... 6
    1.4.4 Qualified Resources .............................................................................................................. 6
2 Overview ....................................................................................................................................... 7
    2.1 Scope ......................................................................................................................................... 8
    2.3 Testing Strategy ........................................................................................................................ 8
3 CSF Assessments ......................................................................................................................... 10
  3.1 Self Assessment ........................................................................................................................... 10
  3.2 CSF Validated ............................................................................................................................. 11
    3.2.1 Testing ......................................................................................................................................... 11
    3.2.2 Submitting Results to HITRUST ........................................................................................... 12
  3.3 CSF Certified ................................................................................................................................ 12
    3.3.1 Testing ......................................................................................................................................... 12
    3.3.2 Submitting Results to HITRUST ........................................................................................... 12
    3.3.3 Granting Certification ............................................................................................................. 12
    3.3.4 De-certification ....................................................................................................................... 13
    3.3.5 Annual Review ......................................................................................................................... 14
    3.3.6 Re-assessments ......................................................................................................................... 14
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Corrective Action Plan</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>Continuous Monitoring</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Appendix A – 2013 Certification Requirements</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Appendix B – CSF Onsite Assessment Submission Documents</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Appendix C – PRISMA Scoring Model</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Appendix D – Rating Scale</td>
<td>25</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Purpose

The purpose of this document is to define the requirements for those organizations conducting an assessment of their security program against the HITRUST Common Security Framework (CSF) to be validated or certified by HITRUST under the CSF Assurance Program. CSF Assessors and those organizations seeking the CSF Assessor designation should also refer to this document to ensure adequate understanding of the process and applicable requirements.

1.2 External References

The following HITRUST documents located on HITRUST Central in the “Downloads” section should be referenced for program background and familiarity with the CSF. This document is focused on addressing the process for an organization to assess its internal security program for validation by HITRUST:

- HITRUST Executive Summary and Introduction
- HITRUST CSF Assessment Methodology
- HITRUST CSF Assessor Requirements

1.3 Background

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

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

The standard requirements, methodology and tools developed and maintained by HITRUST, in collaboration with healthcare and information security professionals, enable both relying and assessed entities to implement a consistent approach to third-party compliance management. Under the CSF Assurance Program, organizations can proactively or reactively, per a request from a relying entity, perform an assessment against the requirements of the 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 in healthcare and other industries, the oversight, vetting and governance provided by HITRUST means greater industry-wide assurances and security.

1.4 Roles and Responsibilities

The following section describes the roles and responsibilities of each organization in the assessment process, including HITRUST, member organizations, and 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.

1.4.1 HITRUST Alliance, Inc.

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

- Maintaining and updating the CSF based on feedback and industry collaboration.
- Supporting CSF Assessors and member organizations in interpreting CSF control objectives, specifications, requirements, assessment procedures, risk factors and standards/regulations cross-references.

1.4.2 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:

- Accrediting and training organizations and individuals who perform the assessments and/or assist member organizations in implementing the CSF.
- Sharing knowledge of security threats/vulnerabilities as well as successful mitigation strategies as provided by CSF Assessors and member organizations.
- Developing and providing approved assessment methodologies and tools for CSF Assessors and member organizations.
- Issuing final validation or certification based on the CSF Assessor’s (or member organization’s where permitted) findings, report, and a corrective action plan as appropriate.
1.4.3 Member Organizations

HITRUST member organizations are those organizations that have adopted the CSF as the security and compliance framework used internally and/or for third parties. Under the CSF Assurance Program, a HITRUST member organization’s responsibilities include:

- Coordinating the performance of assessments and implementing corrective actions and organizational transformations as necessary.
- Funding its CSF Assurance 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 data breaches to HITRUST in accordance with the requirements of the Department of Health and Human Services.

For the purposes of this description “relying” and “assessed” will be used as general descriptors. While covered entities can generally be classified as relying and business associates as assessed, there are many instances where a covered entity is also a business associate with its own security requirements that it must meet as mandated by its customers. Additionally, all organizations must have a mechanism to report to state and federal agencies; a CSF assessment report is one way for organizations to meet such requirements.

1.4.4 Qualified Resources

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

HITRUST defines two classifications of qualified resources: CSF Assessors and CSF Practitioners.

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

CSF Practitioners is a designation reserved for individuals who, as part of a CSF Assessor organization or a HITRUST member organization (e.g., a hospital), have the background, experience, training and understanding to effectively use the CSF. Because CSF Practitioners can be individuals employed by any type of organization, use of the CSF is not limited to performing internal/external assessments. The CSF should also be used as a reference for developing, revising, or maintaining a comprehensive security 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.
2 CSF Assurance Program

2.1 Overview

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

The comprehensiveness of the security requirements for the assessed entity is based on the multiple levels within the 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-assessment questionnaires to on-site analysis/testing performed by a CSF Assessor. The results of the assessment are documented in a standard report with a compliance scorecard and 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 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 CSF assessment allows an organization to communicate to relying entities its compliance with the CSF, and optionally with other requirements such as HIPAA and HITECH. HITRUST reviews the assessment results and CAP to provide added assurance to the external entities relying on the assessed entity’s results.

The CSF Assurance Program effectively establishes trust in health information protection through an achievable assessment and reporting path for organizations of all sizes, complexities and risks. The CSF Assurance Program operates at three levels: Self Assessment, Third-party Validated, or Third-party Certified.

The sections below describe general considerations when performing a self assessment or a third-party assessment. Please refer to the HITRUST CSF Assessment Methodology for more detailed guidance.

2.2 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 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 size. However, in organizations where security control consistency is lacking, the HITRUST member organization and CSF Assessor may determine that a review of all in-scope assets is required to effectively prepare 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 and Planning for and Leveraging MyCSF documents.

2.3 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 is not permitted. 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*. It is ultimately up to the expert judgment of the CSF Assessor to determine the most appropriate testing strategy and the extent of testing to be performed to gain the level of assurance required.
3 CSF Assessments

A CSF assessment provides organizations with a means to assess and communicate their current state of security and compliance with external entities along with a CAP to address any identified gaps. An organization can, using the services of a CSF Assessor or performing a self assessment, conduct an assessment against the CSF and have the results reported by HITRUST under the CSF Assurance Program. The assessed entity is not required by HITRUST to meet all of the security control requirements contained within the CSF. Instead, CSF assessments provide the assessed entity and the relying entity with a snapshot into the current state of security 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, third-party on-site validated assessment, or third-party on-site certified assessment. As suggested by the name, a third-party on-site assessment provides a higher level of assurance since it includes independent testing of the security controls, providing a more complete picture of security and compliance to both the assessed entity and the relying entity.

3.1 Self Assessment

Organizations may choose to self-assess using the standard methodology, requirements, and tools provided under the CSF Assurance Program. HITRUST will perform limited validation on the results of the self-assessment to provide a limited level of assurance to the relying entity without undue burden on the assessed entity.

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 baseline requirements statements will be generated that includes the required 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

Appendix C provides additional detail and guidance on the PRISMA HITRUST model and how HITRUST has incorporated it into its assurance program.

Once the organization has responded to all the requirements statements, it submits the completed questionnaire to HITRUST for review and report generation. The validation of the self-assessment performed by HITRUST will consist of reviewing the completed questionnaire for consistency and ensuring that ambiguous or incomplete responses are addressed. Supporting comments or documentation, if provided, will also be reviewed to determine if the security control requirements are met. If required documentation is missing, it would be noted as such.

3.2 CSF Validated

CSF validated assessments are permitted for organizations of any size or complexity, and consist of more rigorous on-location testing at the entity. The decision to undergo an on-site 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 CSF Validated assessment may be necessary to provide a higher level of assurance to both parties. The process, procedures and rigor for conducting an on-site CSF Validated assessment are very similar to an on-site CSF Certified assessment (see below). The difference is that the assessed entity cannot meet all of the security control requirements contained within the CSF, but still wants to demonstrate that it has many of the CSF required controls in place and has a CAP in place addressing those control categories in need of improvement.

An on-site assessment also utilizes HITRUST’s MyCSF tool. As was the case for a self assessment, the entity being assessed, or the CSF assessor performing the assessment, would begin by completing the risk-based questionnaire in the MyCSF tool. Upon completion of the questionnaire a comprehensive and customized set of baseline requirements statements is generated. The CSF Assessor will work with the assessed entity to respond 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 CSF.

3.2.1 Testing

The CSF Assessor will review any supporting documentation associated with the questions and CSF requirements to ensure it is sufficient to meet the security control requirements and that any missing documentation is gathered or noted as a gap. The CSF Assessor will interview security personnel of the assessed entity to verify that the policies and procedures documented are implemented at the required CSF implementation level and are being followed. The results of the interviews and policy/procedure examinations will be used by the CSF assessor to design and execute tests to validate the responses previously entered. Any previous/recent reviews or assessments should be used by the CSF Assessor to assist in the review and testing process; however, it is ultimately up to the professional judgment of the
CSF Assessor to determine the quality of the tests and whether or not they can comfortably rely on the results or need to do their own independent testing. Additional guidance on conducting a validated assessment and testing can be found in the HITRUST CSF Assessment Methodology document.

3.2.2 Submitting Results to HITRUST

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

3.3 CSF Certified

CSF Certified is a means of confirming that an organization has met all of the certification requirements of the CSF as defined by HITRUST based on industry input and analysis. A CSF Certified assessment leverages the MyCSF tool, the embedded baseline requirements statements and the PRISMA maturity model in the same manner as a CSF Validated assessment, but provides relying entities with greater assurance that their third parties are appropriately managing risk. CSF certification is designed to remove the variability in acceptable security requirements by establishing a baseline defined by the healthcare industry and to be used for the healthcare industry, removing unnecessary and costly negotiations and risk acceptance. By being CSF Certified, an organization is communicating to its business partners and other third-party entities (e.g., state or federal agencies) that sensitive information protection is both a necessity and priority, essential security controls are in place, and management is committed to information security.

3.3.1 Testing

As is true for validated assessments, the assessed entity seeking certification must engage a HITRUST CSF Assessor to perform the assessment. The assessment shall be performed in accordance with the guidance set forth in the HITRUST CSF Assessment Methodology document and will use the same processes and tools as the on-site CSF Validated assessment. An organization does not have to meet those Implementation Requirements where regulatory risk factors are the only drivers of an increased level of control. For example, if the organization is subject to PCI requirements, and the level 3 Implementation Requirement of control 01.xx is driven only by Subject to PCI Compliance; the organization can be certified without meeting the requirements specified at this level for this control.

3.3.2 Submitting Results to HITRUST

Refer to Appendix B for the documents to be submitted to HITRUST following an onsite certified assessment.

3.3.3 Granting Certification

The decision for granting certification to an organization will be based on the testing results of the CSF Assessor and ultimately reviewed, approved and certified by HITRUST.
To be 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\(^2\) for each key control domain documented in MyCSF.

Where certification is granted, certification is valid for two years (24 months) from the certification date as it appears on the certificate on the condition that the continuous monitoring requirements are met.

The development of the 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 received to distinguish the CSF version and certification requirements applicable. Please refer to Appendix A for a complete list of the CSF control specifications required for certification.

The CSF Certified certificate granted will contain the wording “meets the [YEAR] criteria of HITRUST: Specification for healthcare information security management.” 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 certificate shall specify all certified components of the assessed entity.

### 3.3.4 De-certification

Upon discovery of a data security breach, the compromised entity must notify HITRUST if the breach falls under the breach notification requirements of the Department of Health and Human Services. CSF Certified entities that experience a data security breach will undergo an investigation initiated by HITRUST with a 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 CSF Certified organization for a required control, or a misrepresentation of a required control by either the CSF Assessor or 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 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

---

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 six months from the date of certification.

2 Refer to Appendix D for the complete rating scale and definitions of each rating.
compromised entity must bring in a CSF Assessor to review and assess the corrective actions and provide any findings to HITRUST. If no gaps are noted, the 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 CSF controls.

3.3.5 Annual Review

To ensure the assessed entity continues to meet the CSF certification requirements and is remediating any previously identified gaps, HITRUST requires that a CSF Assessor conduct an annual review of the assessed entity. To facilitate that process, the responses to the baseline requirements statements in MyCSF should be reviewed/updated to reflect any changes in controls or control requirements. The review will also address the continuous monitoring activities and CAP developed by the organization. In order to remain CSF Certified, the organization must demonstrate that it has addressed all its remediation actions as agreed in the certified report’s original CAP.

The assessed entity must inform the CSF Assessor of any significant changes in its business policies, practices, processes and controls, particularly if such changes might affect the organization’s ability to continue meeting the required CSF certification security control requirements. Such changes may merit the need for a more extensive re-assessment of the organization and systems. If the CSF Assessor becomes aware of such a change in circumstances, it is the responsibility of the CSF Assessor to report these findings to HITRUST, which will determine whether a re-assessment is needed. The evaluation will take into account the following:

- The nature and complexity of the entity’s operations
- The frequency of changes to the entity’s operations
- The relative effectiveness of the entity’s monitoring and change management controls for ensuring continued compliance with the CSF certification security control requirements

Any acquisition of one entity or by another entity must be communicated to the 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 CSF Certified status as pending until the results of the re-assessment confirm that the changed environment meets the requirements set forth.

Following the annual review, the CSF Assessor will document and submit findings, if any, to HITRUST for evaluation.

3.3.6 Re-assessments

The purpose of the re-assessment is to validate the assessed entity is continuing to comply with the controls of the required CSF Certified controls.
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 defined by the 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 CSF Assurance Program.
4 Corrective Action Plan

The corrective action plan (CAP) prepared by the assessed entity, and the CSF 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 category of the information systems, the direct effect the vulnerability has on the overall security posture of the information systems, and the requirements for CSF certification.

The CAP should include, at a minimum, a weakness identifier, description of the weakness, CSF control mapping, point of contact, resources required (dollars, time, and/or personnel), scheduled completion date, milestones with completion dates, changes to milestones, how the weakness was identified (assessment, CSF Assessor, date), current status, comments, and risk level. The CSF Assessor must review the CAP to evaluate the effectiveness of the remediation strategy, provide recommendations, and document any findings for submission to HITRUST.
5 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 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 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 risk analysis for planned or actual changes to an operational environment or an information system, ongoing selective evaluation of security controls, and frequent interaction between information systems management and the security team.

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

The security team 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 – 2013 Certification Requirements

The top issues the industry identified as resulting in the most severe breaches and loss of covered information are:

- Lack of a formal information protection program to identify and manage risk
- Incomplete accounting and configuration control of information assets
- Insecure and/or unauthorized removable/transportable media and laptops (internal and external movements)
- Insufficient or otherwise ineffective use of encryption and/or key management
- Insecure and/or unauthorized external electronic transmissions of covered information
- Poor management of internal and third party identities and their access privileges
- Insecure and/or unauthorized remote access by internal and third party personnel
- Insider snooping and data theft
- Malicious code and inconsistent implementation and update of prevention software
- Inadequate and irregular information security awareness for the entire workforce
- Lack of consistent network isolation between internal and external domains
- Insecure and/or unauthorized implementation of wireless technology
- Failure to obtain appropriate assurances around third party / vendor security practices
- Lack of consistent service provider, third party and product support for information security
- Insecure web development and applications
- Ineffective password management and protection
- Improper sanitization and disposal of electronic and hardcopy media
- Failure to adequately secure facility perimeters and sensitive areas within the facility.

In consideration of the above issues, the Control Specifications of the CSF required for 2013 certification are:

<table>
<thead>
<tr>
<th>Required for HITRUST Certification 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>01.a Information Security Management Program*</td>
</tr>
<tr>
<td>01.a Access Control Policy</td>
</tr>
<tr>
<td>01.b User Registration</td>
</tr>
<tr>
<td>01.d User Password Management</td>
</tr>
<tr>
<td>01.f Password Use</td>
</tr>
<tr>
<td>01.h Clear Desk and Clear Screen Policy</td>
</tr>
<tr>
<td>01.i Policy on Use of Network Services</td>
</tr>
<tr>
<td>01.j User Authentication for External Connections</td>
</tr>
<tr>
<td>01.m Segregation in Networks</td>
</tr>
<tr>
<td>01.n Network Connection Control</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>01.o Network Routing Control</td>
</tr>
<tr>
<td>01.q User Identification and Authentication</td>
</tr>
<tr>
<td>01.r Password Management System</td>
</tr>
<tr>
<td>01.v Information Access Restriction</td>
</tr>
<tr>
<td>01.w Sensitive System Isolation</td>
</tr>
<tr>
<td>01.x Mobile Computing and Communications</td>
</tr>
<tr>
<td>01.y Teleworking</td>
</tr>
<tr>
<td>02.a Roles and Responsibilities</td>
</tr>
<tr>
<td>02.d Management Responsibilities</td>
</tr>
<tr>
<td>02.e Information Security Awareness, Education, and Training</td>
</tr>
<tr>
<td>02.f Disciplinary Process</td>
</tr>
<tr>
<td>02.i Removal of Access Rights</td>
</tr>
<tr>
<td>03.a Risk Management Program Development*</td>
</tr>
<tr>
<td>03.b Performing Risk Assessments</td>
</tr>
<tr>
<td>03.c Risk Mitigation</td>
</tr>
<tr>
<td>04.a Information Security Policy Document</td>
</tr>
<tr>
<td>04.b Review of the Information Security Policy</td>
</tr>
<tr>
<td>05.a Management Commitment to Information Security</td>
</tr>
<tr>
<td>05.b Information Security Coordination</td>
</tr>
<tr>
<td>05.i Identification of Risks Related to External Parties</td>
</tr>
<tr>
<td>05.k Addressing Security in Third Party Agreements</td>
</tr>
<tr>
<td>06.d Data Protection and Privacy of Covered Information</td>
</tr>
</tbody>
</table>

* New for 2013
Appendix B – CSF Onsite Assessment Submission Documents

The following documentation is required to be submitted by the CSF Assessor to HITRUST for on-site CSF Third-party Validated and Certified assessments:

- A completed MyCSF Baseline Questionnaire
- 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

For instances where an organization has requested a compliance scorecard for one or more of the authoritative sources incorporated in the CSF (other than HIPAA which is automatically included), the MyCSF Comprehensive Assessment questionnaire must be completed and submitted with documentation of testing performed for each CSF control.
Appendix C – PRISMA Scoring Model

The effectiveness of an organization’s control implementation is based on a model described in NIST Interagency Report (IR) 7358, Program Review of Information Security Management Assistance (PRISMA), which uses five levels to help organizations determine the maturity of one or more requirements in a CSF Control Specification: Policy, Procedures, Implemented, Measured, and Managed.

The following table provides a generic set of questions that should be considered when evaluating a requirements statement at each level of the model:

<table>
<thead>
<tr>
<th>Level</th>
<th>Generic Evaluation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Policy</td>
<td></td>
</tr>
</tbody>
</table>
  • Do formal, up-to-date policies or standards exist that contain “shall” or “will” statements for each element of the requirement statement??  
  • Do the policies and standards that exist for each element of the requirement statement cover all major facilities and operations for the organizations and/or systems/assets in scope for the assessment?  
  • Are the policies and standards that exist for each element of the requirement statement approved by management and communicated to the workforce? |
| 2 - Procedures |  
  • Do formal, up-to-date, documented procedures exist for the implementation of each element of the requirement statement?  
  • Do the procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed? |
| 3 - Implemented |  
  • Are procedures for the implementation of each element of the requirements statement communicated to the individuals who are required to follow them?  
  • Is each element of the requirements statement implemented in a consistent manner everywhere that the procedure applies?  
  • Are ad hoc approaches that tend to be applied on an individual or on a case-by-case basis discouraged? |
<table>
<thead>
<tr>
<th>Level</th>
<th>Generic Evaluation Criteria</th>
</tr>
</thead>
</table>
| 4 – Measured | • Are self-assessments, audits and/or tests routinely performed and/or metrics collected to evaluate the adequacy and effectiveness of the implementation of each element of the requirements statement?  
• Are evaluation requirements, including requirements regarding the type and frequency of self-assessments, audits, tests, and/or metrics collection documented, approved and effectively implemented?  
• Does the frequency and rigor with which each element of the requirements statement is evaluated depend on the risks that will be posed if the implementation is not operating effectively? |
| 5 - Managed | • Are effective corrective actions taken to address identified weaknesses in the elements of the requirements statement, including those identified as a result of potential or actual information security incidents or through information security alerts?  
• Do decisions around corrective actions consider cost, risk and mission impact?  
• Are threats impacting the requirements periodically re-evaluated and the requirements adapted as needed? |

When used with the Illustrative Procedures available in MyCSF, these questions provide additional context for the evaluation of specific requirements statements in a Baseline or Comprehensive Assessment (available in mid-2013).

The HITRUST control maturity model also incorporates the following 5-point compliance scale which is used to score each level in the model: Non-Compliant (NC), Somewhat Compliant (SC), Partially Compliant (PC), Mostly Compliant (MC) and Fully Compliant (FC).

<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Compliant (NC)</td>
<td>Very few if any of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 0%.</td>
</tr>
<tr>
<td>Somewhat Compliant (SC)</td>
<td>Some of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 25%.</td>
</tr>
<tr>
<td>Partially Compliant (PC)</td>
<td>About half of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 50%.</td>
</tr>
<tr>
<td>Mostly Compliant (MC)</td>
<td>Many but not all of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 75%.</td>
</tr>
</tbody>
</table>
Score | Description
--- | ---
**Fully Compliant (FC)** | Most if not all of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 100%.

Example:

An external assessor wants to evaluate the following the encryption component of the following requirement statement, which is derived from CSF control 01.x:

*Mobile computing devices are protected at all times by access controls, encryption, virus protections, host-based firewalls, secure configuration, and physical protections.*

The academic hospital requires by policy that all portable computing devices, whether a laptop or a smartphone, be encrypted if the device is used to access covered information. The organization gets credit for full compliance with the policy requirement. The organization has formal procedures in place to ensure Windows-based laptops and all smartphones are encrypted but have yet to establish procedures for the encryption of Mac laptops due to resistance from the research community. As they can demonstrate all Windows-based laptops and smartphones were encrypted when the capability was rolled out earlier in the year, the hospital scores mostly compliant for procedures and implementation. The management console used by end-user devices and the mobile device management console for smartphones both have the capability to report on the encryption status for these devices but the reports are seldom run since the managers’ bonuses are tied to meeting operational service levels and executive leadership lost interest once the encryption project was completed for Windows-based devices, which accounts for 95% of their total environment. The organization gets a somewhat compliant score for “honorable mention” and noncompliance for management, as the organization does not use this information to evaluate and manage the effectiveness of the encryption implementation. So based on the facts are presented, the scoring might look as follows for this requirement statement:

<table>
<thead>
<tr>
<th>Level (Points)</th>
<th>NC</th>
<th>SC</th>
<th>PC</th>
<th>MC</th>
<th>FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy (25)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures (25)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implemented (25)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measured (15)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managed (10)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The compliance scale is evenly weighted (0, 25, 50, 75, 100) but the PRISMA scores for each level are weighted differently (25, 25, 25, 15, 10). Essentially the last two levels are combined (for a total of 25 points) to address the concept of “one can’t manage what one can’t measure” and still account for the
fact that not all organizations actively manage their controls even though they may actively measure their effectiveness. For example, an organization may perform a root cause analysis after every security incident but fail to take appropriate measures based on the results.

In this example the academic hospital would score the following for the encryption component of the requirement: \( (1.0)(25) + (.75)(25) + (.75)(25) + (.25)(15) + (0.0)(10) = 66.25 \).

Once the control requirements are assessed using HITRUST’s PRISMA-based maturity model, the scores can be aggregated across all the requirements of a particular control or multiple controls in a domain. These estimates can also be used to support reporting for specific controls or domains for one or more organizations, type(s) of business units across multiple organizations, one or more information systems, or type(s) of information systems. Estimates can also be used to generate one or more Scorecards, such as for HIPAA or Cybersecurity.
Appendix D – Rating Scale

As used in the HITRUST CSF Assurance Program, the PRISMA-based maturity scores are converted to a 15-level maturity rating as follows:

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>1-</th>
<th>1</th>
<th>1+</th>
<th>2-</th>
<th>2</th>
<th>2+</th>
<th>3-</th>
<th>3</th>
<th>3+</th>
<th>4-</th>
<th>4+</th>
<th>5-</th>
<th>5</th>
<th>5+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cutoff PRISMA Score</td>
<td>&lt; 10</td>
<td>&lt; 19</td>
<td>&lt; 27</td>
<td>&lt; 36</td>
<td>&lt; 45</td>
<td>&lt; 53</td>
<td>&lt; 62</td>
<td>&lt; 71</td>
<td>&lt; 79</td>
<td>&lt; 83</td>
<td>&lt; 87</td>
<td>&lt; 90</td>
<td>&lt; 94</td>
<td>&lt; 98</td>
</tr>
</tbody>
</table>

Using the example in Appendix C, a score of 66.25 for mobile device encryption would result in a maturity rating of a “3”, which essentially means that most if not all of the encryption requirements are defined in a policy or standard and supported with organizational procedures, and many if not most of the devices are encrypted as required by the CSF.

However, one should note that the aggregated scores simply provide “likelihood estimators” for the probability that one or more controls might fail to operate as intended. When used for CSF validation and certification, these aggregated scores provide guidelines for HITRUST’s quality assurance evaluation of the assessment approach and evidence obtained to support the scores. Other factors such as a significant deficiency in the implementation of one or more controls could prevent an organization from becoming CSF Certified even though they score a “3-“ or better in every assessment domain.

General definitions for each of the 15 maturity ratings are provided in the table below:

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Rating Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1-</td>
<td>Few if any of the control specifications included in the assessment scope are defined in a policy or standard and may not be implemented as required by the HITRUST CSF.</td>
</tr>
<tr>
<td>Level 1</td>
<td>Many of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 1+</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 2-</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but few if any of the requirements are supported with organizational procedures or implemented as required by the CSF.</td>
</tr>
<tr>
<td>Maturity Level</td>
<td>Rating Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Level 2</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, many of the requirements are supported with organizational procedures, but few if any are implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 2+</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, but few if any are implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 3-</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and some are implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 3</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and many are implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 3+</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported with organizational procedures, and implemented as required by the CSF.</td>
</tr>
<tr>
<td>Level 4-</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and some of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST CSF.</td>
</tr>
<tr>
<td>Level 4</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and many of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST CSF.</td>
</tr>
<tr>
<td>Level 4+</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured to ensure they function as intended and as required by the HITRUST CSF.</td>
</tr>
<tr>
<td>Level 5-</td>
<td>Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and some are actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.</td>
</tr>
<tr>
<td>Maturity Level</td>
<td>Rating Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Level 5</td>
<td><strong>Most if not all</strong> of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and <strong>many</strong> are actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.</td>
</tr>
<tr>
<td>Level 5+</td>
<td><strong>Most if not all</strong> of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, routinely measured, and actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.</td>
</tr>
</tbody>
</table>