CSF Assurance Program FAQ

1509 - v1.0

What is the HITRUST CSF Assurance Program?

The HITRUST CSF Assurance program is a common, standardized methodology to effectively and consistently measure compliance and risk via simplified information collection and reporting, consistent testing procedures and scoring, and demonstrable efficiencies and cost-containment; and additional assurances around the accuracy, consistency and repeatability of assessments due to the use of pre-qualified professional services firms—all of which is designed to meet the unique regulatory and business needs of the healthcare industry. In short, it is a risk-based approach to selecting HITRUST CSF controls for assessment, including management oversight of the assessment. The HITRUST CSF Assurance Program delivers simplified compliance assessment and reporting that addresses multiple federal, state and industry requirements for both covered entities and their business associates.

References:* ***HITRUST CSF Assurance Program Brochure* *and the* ***CSF Assurance Program Requirements***

What are the various types of CSF Assessments

HITRUST offers two types of CSF Assessments: a self-assessment and a validated assessment.

Self-assessment allows organizations to self-assess using the standard methodology, requirements, and tools provided under the CSF Assurance Program. HITRUST will then perform limited validation on the results of the self-assessment to provide a limited level of assurance to the relying entity.

Validated assessment is conducted by a HITRUST Certified CSF Assessor. The CSF Assurance methodology is used and the controls are scored accordingly. Assessments meeting or exceeding the current CSF Assurance scoring requirements for certification will be indicated as CSF Certified on the certification report.

References:* ***What Assessment is Right for Me?* *and* ***CSF Assurance Program Requirements***

Is a HITRUST certification assessment more expensive than comparable assessments?

No, and this is a common misconception and in many cases the overall assessment costs associated with information security and privacy assessments are less than other 3rd party assessments. The alignment between the HITRUST CSF and CSF Assurance programs allows a single CSF Assessment report to support multiple objectives, such as a HIPAA risk assessment and an assessment against the NIST Cybersecurity Framework, and in addition the same report can be accepted by external parties (such as business partners, government agencies) reducing the costs associated with multiple assessments.

For a fair comparison, one should consider various factors such as:

- **Scope of the Assessment:** Are both assessments reviewing the same scope?
- **Applicability of the Control Requirements to the Environment:** Are the controls requirements applicable to the organization or scope of assessment? Are they prescriptive and do they take into account relevant risk factors?
- **Audit Ability:** Does the framework have audit procedures to ensure consistency of assessment?
- **Level of Assurance:** How well is the process to ensure the control requirements implemented?
- **Caliber of Organization Performing Assessment:** Is It being performed by a 3rd party? What are the qualifications of the firm performing the assessment?

References:* ***HITRUST CSF Assurance Program Brochure* *and the* ***CSF Assurance Program Requirements***

What is the length of time it takes to become HITRUST CSF Certified?

CSF Certification can be achieved when all 64 required controls are fully implemented in the scoped environment (2015 CSF v7 requirement). The total amount of time it can take an organization to become certified is therefore dependent on its initial readiness level and the amount of remediation needed to fully implement all the requirements in scope for the assessment. Most organizations will perform at least one self-assessment to gauge their readiness for certification and, once an organization is comfortable that they will meet the certification requirements, they will hire a CSF assessor to perform a validated assessment. These independent assessments can take anywhere from 2-8 weeks on average depending on the size and complexity of the organization and the scoped environment, and it can take an additional 6 weeks for the validated assessment to be processed and certification awarded by HITRUST. In general, it can take up to 3-4 month to complete the assessment and obtain certification once an organization is ready.

Reference:* ***CSF Assurance Program Requirements*

Who will accept HITRUST CSF Assurance Reports?

Many organizations accept CSF Assurance reports as a means of evaluating a business partner's privacy and security controls and in fact a growing number of organizations require their business partners obtain a CSF Certification..

Reference:* ***HITRUST CSF Assurance Program Brochure*

If I'm HITRUST CSF Certified, does that mean I'm HIPAA compliant?

In principle yes, but it is not black and white. To be HIPAA-compliant, an organization must conduct a risk analysis and implement a reasonable and appropriate set of information safeguards—aka information security controls—to provide for the adequate protection of ePHI against all reasonably anticipated threats. In practice, organizations that want to demonstrate HIPAA compliance must generally show that it has addressed each standard and implementation specification in the Security Rule, including risk analysis. Organizations must therefore design or select multiple information security controls to provide the level of prescription necessary for implementation in the system or within the organization.

HITRUST helps organizations select these controls via its extensive mapping of the CSF controls to the HIPAA Security Rule's standards and implementation specifications. Many of the HIPAA requirements are mapped to multiple controls, and the CSF controls themselves consist of multiple, specific protection requirements contained in multiple levels. By implementing the HITRUST CSF control requirements that are applicable to an organization based on its specific organizational, system and regulatory risk factors, each and every standard and implementation specification in the Security Rule is addressed in a very complete and robust way.

However, CSF certification is based on an assessment of a subset of the controls an organization is expected to implement. These controls were selected based on an analysis of past breach data and the need to address each and every standard and implementation specification in the HIPAA Security Rule. NIST supports the use of such targeted assessments to answer specific questions like this, and the use of a targeted assessment for CSF certification ensures relying organizations receive reasonable assurances at a reasonable cost.

DHHS specifically references HITRUST and the CSF with respect to risk management and risk assessment in its Guidance on Risk Analysis Requirements under the HIPAA Security Rule, and OCR has stated entities with a strong compliance program in place, with the help of a credentialing/accreditation program or on its own, would have that taken into account when determining past compliance. Implementation of the CSF as the basis for an organization's information protection program and subsequent use of CSF validated or certified assessments has been previously accepted by OCR as evidence of its compliance with the HIPAA Security Rule, assuming the assessment addresses the appropriate scope relevant to OCR's audit or investigation. The CSF and CSF Assurance Program has also been used in past resolution agreements with OCR.

References:* ***HIPAA is King* *(article) and* ***HITRUST CSF Streamlines and Enhances NIST to Achieve HIPAA Compliance*** *(article)*

CSF Assurance Program FAQ

1509 - v1.0

How many organizations have completed a HITRUST CSF Assessment?

23,000 CSF Assessments have been performed in the last three years with 10,000 CSF Assessments in 2014 alone. HITRUST anticipates a continued demand for CSF certification due to third party assurance requirements from several major health organizations, the SECURETexas program and requests for combined CSF-SOC2 reports.

Reference:* ***HITRUST Key Programs and Services 2015*

What is the process for an organization to achieve HITRUST CSF Certification?

Before starting the Certification process, HITRUST recommends a self-assessment or readiness assessment be performed to prepare organizations for the validated assessment. To begin the Certification process, please select a HITRUST Assessor. Once you select an Assessor, you will need to purchase a validated assessment from HITRUST. Complete the validated assessment using the MyCSF tool and then the Assessor will perform the validation/audit work. Please note access to the MyCSF is granted for 90 days. Once the Assessor work is complete, please submit to HITRUST for review. HITRUST will create a report and, depending on the scores in the report, will issue a letter of certification.

Reference:* ***CSF Assurance Program Requirements*

How can my organization utilize the CSF framework for a SOC 2 report?

HITRUST and AICPA are collaborating on the mapping of HITRUST CSF controls to AICPA Trust Principles and Criteria, and work has been completed on the Trust Services Principles for Security, Confidentiality and Availability. Subsequently, any AICPA firm can perform a SOC 2 audit leveraging the CSF framework. This audit allows the client to receive HITRUST Certification and a SOC 2 report, a combined format for which AICPA and HITRUST are currently in the process of developing. HITRUST has also submitted comments on the recent exposure draft of AICPA's Proposed Revision of Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy and anticipates mapping to the privacy principle in 2016.

References:* ***HITRUST and AICPA Develop a "SOC 2 for HITRUST" Converged Reporting Model to Improve Efficiency and Reduce Costs* *(Deloitte Article), and* ***SOC 2 to HITRUST Mapping***