HITRUST CSF Assurance Program

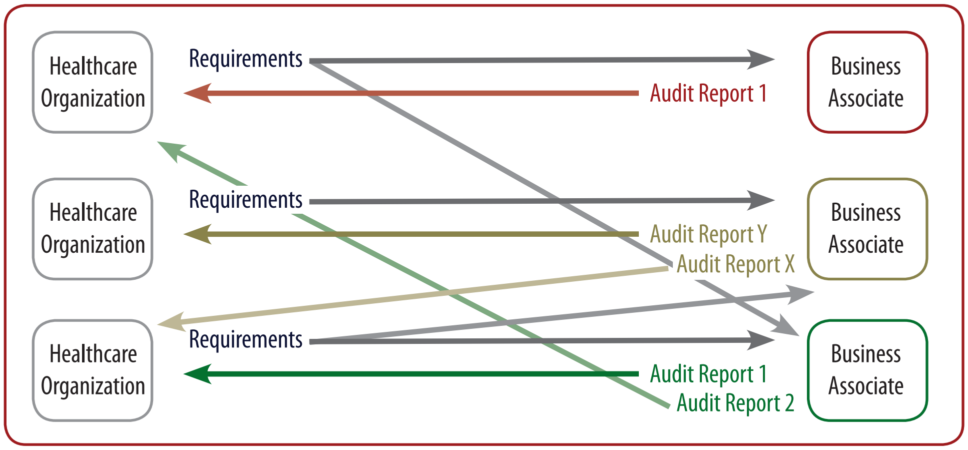
Common healthcare industry approach for assessing security and reporting compliance

Background and challenges

Compliance requirements for healthcare organizations and their business associates are becoming more stringent as organizations face multiple and varied assurance requirements from internal and external auditors and other third parties such as health information organizations (HIOs) and federal and state agencies. The increasing pressure and penalties associated with the enforcement efforts of HIPAA and the HITECH Act have led to a growing need to simplify the compliance process for the healthcare industry. As breaches become more costly, the need for increased due diligence by all parties to ensure that essential security and privacy controls are in place is greater now than ever before.

Unfortunately, the existing model of unique and inconsistent requirements and processes to validate compliance and mitigate risks associated with third parties is leading to an inordinate level of effort being spent on the negotiation of requirements, data collection, assessment, and reporting. This is costly to both healthcare organizations[1] and their business associates, detracting from the implementation of an effective overall risk management program.

Current state of reporting



Improving risk management while reducing cost and complexity

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 their business associates can improve efficiencies and reduce the number and costs of security assessments. The oversight and governance provided by HITRUST support a process whereby organizations can trust that their third parties have essential security controls in place.

[1] Certain healthcare organizations may function both as a healthcare organization (i.e., covered entity) and a business associate. The CSF Assurance Program meets the reporting needs of the organization as a covered entity (i.e., internal and regulatory stakeholders) and as a business associate (i.e., customer requirements).

HITRUST
Health Information Trust Alliance

At a high level, both healthcare organizations and their business associates experience issues leading to greater cost, complexity, and risk such as:

- Broad range of inconsistent expectations with respect to security
- Maintenance and tracking of disparate requirements and corrective actions
- Expensive and time-intensive audits occurring at random intervals
- Inability to consistently and effectively report and communicate between organizations
- Lack of assurance that risk is appropriately managed

The wide range of assessment and reporting requirements has contributed to inefficiencies and exposure that will only be resolved with the standardization and adoption of a common, industry-wide approach.

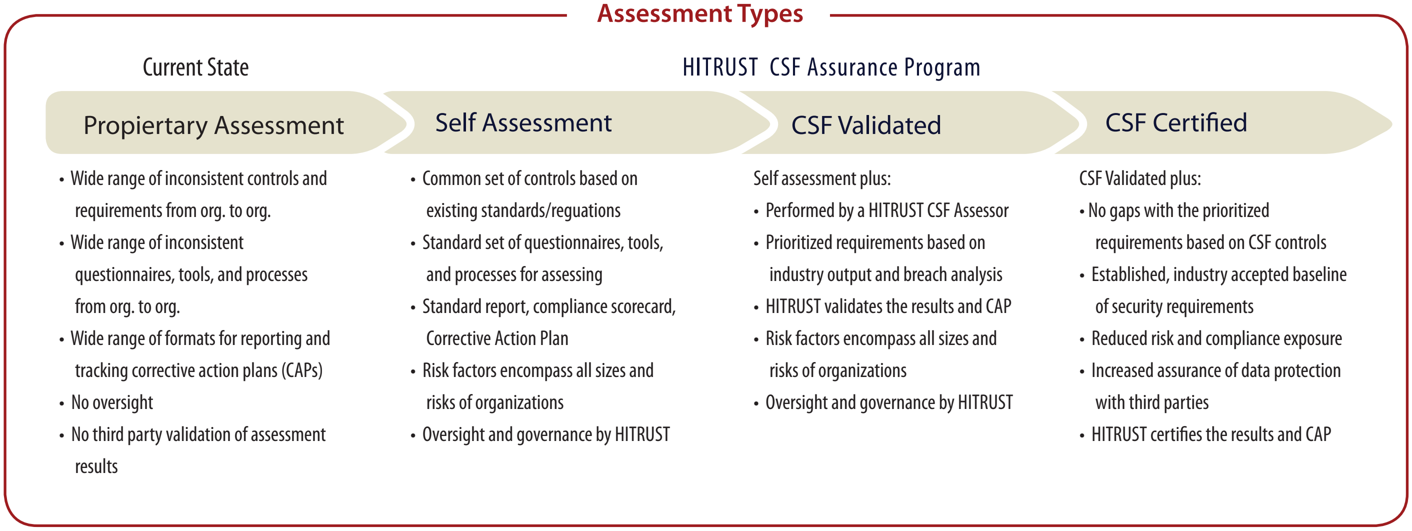
Incremental path to compliance

An integral component to achieving HITRUST's goal to advance the healthcare industry's protection of health information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST Common Security Framework (CSF). The CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon healthcare organizations, including federal (e.g., HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The CSF was developed in collaboration with healthcare and information security professionals and is already being widely adopted by leading healthcare payers, providers, and state exchanges as their security framework.

HITRUST has developed the common requirements, methodology, and tools that enable both healthcare organizations and their business associates to take a consistent and incremental approach to managing compliance: the HITRUST CSF Assurance Program. This program is the mechanism that allows healthcare organizations and business associates to assess and report against multiple sets of requirements. Unlike other programs in healthcare and in other industries, the oversight, vetting and governance provided by HITRUST and the CSF Assurance Committee affords greater assurances and security across the industry.

By utilizing the program, organizations can proactively or reactively, per a request, perform an assessment against the requirements of the CSF. This single assessment will give an organization insight into its security program and state of compliance against the various requirements incorporated into the CSF. For organizations that are already striving to implement the information protection controls defined in the CSF, the program allows them to receive immediate and incremental value from the CSF through common reporting tools and processes.

Assessment Types



Current State	HITRUST CSF Assurance Program		
Propiertary Assessment	Self Assessment	CSF Validated	CSF Certified
• Wide range of inconsistent controls and requirements from org. to org. • Wide range of inconsistent questionnaires, tools, and processes from org. to org. • Wide range of formats for reporting and tracking corrective action plans (CAPs) • No oversight • No third party validation of assessment results	• Common set of controls based on existing standards/reguations • Standard set of questionnaires, tools, and processes for assessing • Standard report, compliance scorecard, Corrective Action Plan • Risk factors encompass all sizes and risks of organizations • Oversight and governance by HITRUST	Self assessment plus: • Performed by a HITRUST CSF Assessor • Prioritized requirements based on industry output and breach analysis • HITRUST validates the results and CAP • Risk factors encompass all sizes and risks of organizations • Oversight and governance by HITRUST	CSF Validated plus: • No gaps with the prioritized requirements based on CSF controls • Established, industry accepted baseline of security requirements • Reduced risk and compliance exposure • Increased assurance of data protection with third parties • HITRUST certifies the results and CAP

How the process works

Healthcare organizations require different levels of assurance based on the risk of the relationship with each business associate. The levels of assurance include self-assessments for small and low-risk business associates and on-site analysis and testing for associates that present the most risk to organizations.

The results of the assessment are documented in a standard report accompanied by a compliance scorecard. Remediation activities are included in a corrective action plan (CAP) and can be regularly tracked. Once vetted by HITRUST, the assessed entity can leverage the single assessment to report to multiple internal and external parties (e.g., state and federal agencies, HIOs, customers, healthcare organizations, business associates), saving time and containing costs.

Assisting in the documentation of findings and preparation of reports are CSF Assessors - those organizations uniquely qualified to deliver services under the CSF Assurance Program. Using CSF Assessors ensures that highly trained security professionals knowledgeable in healthcare and the CSF are accurately reporting findings to HITRUST, providing the increased level of assurance that relying entities demand. The CSF Assurance Program enables trust in health information protection through an efficient and manageable approach by defining an achievable path: Self Assessment, CSF Validated and/or CSF Certified. All leverage the same tools and processes, but provide different levels of assurance.

CSF Assurance Committee

The CSF Assurance Committee is responsible for the creation and management of the policies and procedures that ensure the quality, accuracy, and fairness of assessments and the resulting reports. The committee also serves as an arbitrator to help resolve any issues between an organization being assessed and its CSF Assessor.

Self Assessments

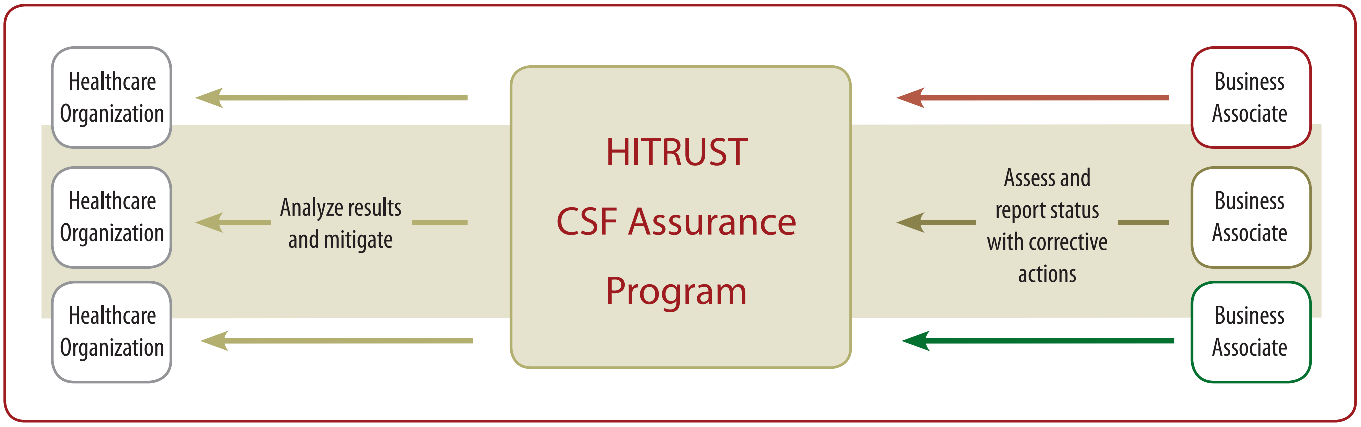
Self assessments can be conducted by utilizing the tools and methodologies of the CSF Assurance Program. The assessment results are then prepared by HITRUST for reporting to third parties. The self-assessment option removes any potential barriers for organizations that lack the resources for an onsite assessment, but nonetheless must still implement data protection controls, maintain HIPAA/ HITECH compliance, and report to external parties.

CSF Validated

CSF Validated allows both healthcare organizations and their business associates to realize the benefits of more assurance with fewer resources, which is achieved by aligning with the CSF and leveraging of common reporting processes and tools. There are three levels of validation:

CSF Validated assessments are conducted by CSF Assessors and allow both healthcare organizations and their business associates to realize the benefits of more assurance with fewer resources, which is achieved by aligning with the CSF and leveraging of common reporting processes and tools.

HITRUST CSF Assurance Program



These assessments involve onsite interviews, documentation review and system testing and provide a greater level of assurance, meant for those organizations with higher impact and higher risk relationships.

CSF Certified

CSF Certified is a means of recognizing that an organization has met all of the certification requirements of the CSF as defined by the industry. Utilizing the same tools, processes and reporting components as CSF Validated, CSF Certified provides internal and external parties with the greatest level of assurance that an organization is appropriately managing risk by meeting those industry-defined and accepted security requirements.

Certification is designed to remove the variability in acceptable security requirements by establishing a baseline defined by and to be used for the healthcare industry, removing unnecessary and costly negotiations and risk acceptance. By becoming CSF Certified, an organization is communicating to external parties that sensitive information protection is both a necessity and priority, essential security controls are in place, management is committed to information security, and the risk of a breach has been reduced to a reasonable level.

Why HITRUST CSF Assurance?

The HITRUST CSF Assurance Program establishes a common approach for addressing industry and regulatory requirements and helps keep compliance costs and risk exposures from spiraling out of control.

- Reduced costs and complexity. Through the adoption of a common set of security objectives and assessment processes, the CSF Assurance Program streamlines how healthcare organizations manage business-associate compliance. Business associates can assess once and report to their many constituents, while healthcare organizations and other external parties benefit from a more complete and effective assessment process.
- Managed risk. Through a commercially reasonable process, organizations will achieve increased insight into their internal and third-party risks. By freeing resources from reacting to new requirements and audits, organizations can take a proactive approach focusing on the other building blocks of an effective security management program.
- Simplified compliance. Organizations benefit from a consistent and efficient approach for reporting compliance with internal stakeholders, HIPAA, HITECH, state, and business associates.

When an organization asks their business associates or external parties to report or accept assessment results using the CSF Assurance Program, they do so with confidence in the comprehensiveness of both the report and process. They are also aware of the fact that the report aligns with the existing regulatory and statutory requirements placed upon healthcare organizations as well as internationally recognized standards such as ISO 27001 and 27002. For business associates and other organizations being assessed, this means one assessment encompassing important compliance requirements such as HIPAA and HITECH that can be consistently reported to various customers. For healthcare organizations and other external parties, this means an industry-accepted process based on a comprehensive set of requirements to validate the security program of business associates. Because HITRUST continually oversees the process and vets the assessment results, all parties benefit from reduced time, resources and confusion regarding the reporting and monitoring of compliance.

With the establishment and acceptance of the CSF and related tools, HITRUST is uniquely positioned to support the healthcare community and their business partners in adopting common assessment and reporting processes. With HITRUST's guidance and oversight, healthcare organizations and business associates, supported by the CSF Assessor organizations, are able to realize the benefits of a single, complete risk and compliance review. There is simply no other practical option that is sustainable, helps contain costs, and actually improves security compliance over time.

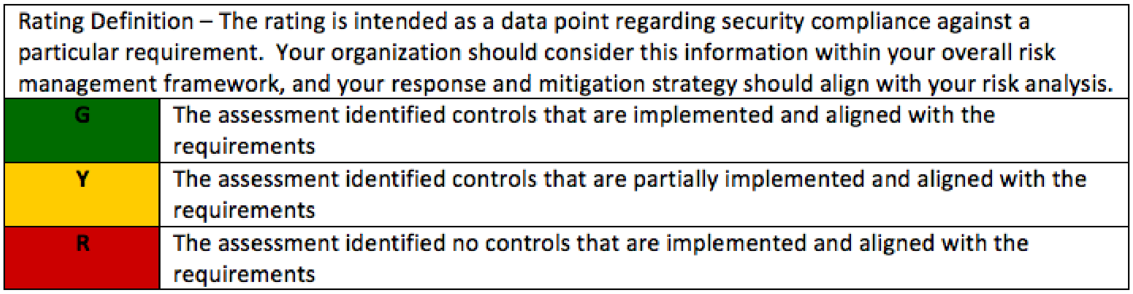
Learn more

Please call 469.269.1110 for more information on the HITRUST CSF Assurance Program and CSF Assessors or visit www.HITRUSTalliance.net/assurance.

MyCSF

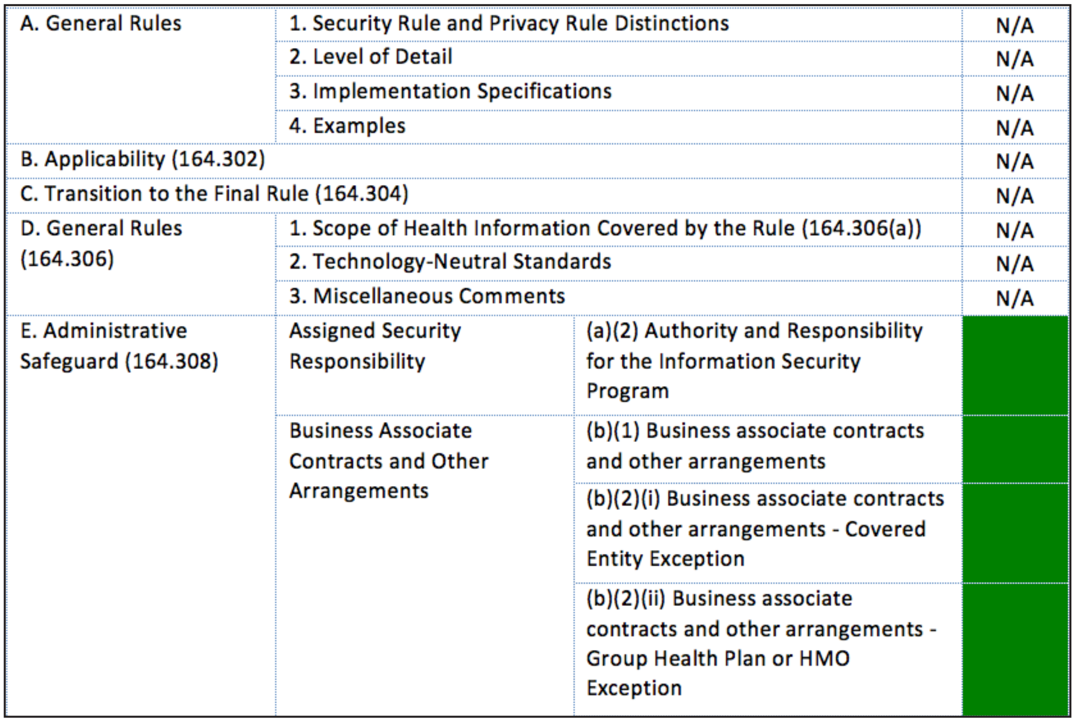
Instrumental to the CSF Assurance Program is the user-friendly MyCSF tool which provides healthcare organizations of all types and sizes with a secure, Web-based solution for accessing the CSF, performing assessments, managing remediation activities, and reporting and tracking compliance. Managed and supported by HITRUST, MyCSF provides organizations with up-to-date content, accurate and consistent scoring, reports validated by HITRUST, and benchmarking data unavailable anywhere else in the industry, thus going far beyond what a traditional GRC tool can provide. Learn more about MyCSF.

Sample Compliance Scorecard Index



Rating Definition – The rating is intended as a data point regarding security compliance against a particular requirement. Your organization should consider this information within your overall risk management framework, and your response and mitigation strategy should align with your risk analysis.	
G	The assessment identified controls that are implemented and aligned with the requirements
Y	The assessment identified controls that are partially implemented and aligned with the requirements
R	The assessment identified no controls that are implemented and aligned with the requirements

HIPAA Security Rule Scorecard Example:



A. General Rules	1. Security Rule and Privacy Rule Distinctions		N/A
	2. Level of Detail		N/A
	3. Implementation Specifications		N/A
	4. Examples		N/A
B. Applicability (164.302)			N/A
C. Transition to the Final Rule (164.304)			N/A
D. General Rules (164.306)	1. Scope of Health Information Covered by the Rule (164.306(a))		N/A
	2. Technology-Neutral Standards		N/A
	3. Miscellaneous Comments		N/A
E. Administrative Safeguard (164.308)	Assigned Security Responsibility	(a)(2) Authority and Responsibility for the Information Security Program	🟩
	Business Associate Contracts and Other Arrangements	(b)(1) Business associate contracts and other arrangements	🟩
		(b)(2)(i) Business associate contracts and other arrangements - Covered Entity Exception	🟩
		(b)(2)(ii) Business associate contracts and other arrangements - Group Health Plan or HMO Exception	🟩

Vehicle for monitoring compliance of third parties

Healthcare organizations must have confidence in their business associates' ability to implement a privacy and security program that safeguards protected health information. More often than not, it is the healthcare organization's name that is used in public reports of a data privacy breach and other high-profile violations; thus, making the business-associate relationship a critical component in protecting their reputation and managing compliance efforts. The CSF Assurance Program provides healthcare organizations with a standard, cost-efficient means to assess the security program of business associates and get the results as required by HIPAA. By using the CSF Assurance Program, organizations are no longer left to work in isolation to develop unique requirements that consume time and money and are not accepted industry-wide.

CSF Assessors

A component of the HITRUST CSF Assurance Program is the utilization of professional services organizations to provide the assessment and remediation services. These organizations must meet certain criteria initially and continue to maintain their standing to receive HITRUST's approval to perform any CSF Assurance Program related work. Information security experience and technical competence with healthcare organizations (e.g., medical facilities/providers, health plans/payers, clearinghouses) are among the criteria.

Individuals from CSF Assessor organizations must also attend a specialized training course and pass a comprehensive exam to become a HITRUST Practitioner, a designation of technical competence in healthcare security, risk management, and use of the CSF. The purpose of the criteria established by HITRUST is to provide an added level of assurance that the assessment is conducted in a comprehensive and appropriate manner. To learn more, visit www.HITRUSTalliance.net/assessors.

Access your copy of the CSF

The HITRUST CSF is available through both MyCSF and HITRUST Central, the industry's first managed online community for health information security professionals.

The HITRUST CSF:

- Leverages existing, globally recognized standards, including HIPAA, NIST, ISO, PCI, FTC, and Cobit
- Scales according to type, size, and complexity of an implementing organization
- Provides prescriptive requirements to ensure clarity
- Follows a risk-based approach offering multiple levels of implementation requirements determined by risks and thresholds
- Allows for the adoption of alternate controls when necessary
- Evolves according to user input and changing conditions in the healthcare industry and regulatory environment

In addition to providing access to the CSF, HITRUST Central includes a blog, question and answer forums, downloads, and group collaboration spaces. To learn more and to register, visit www.hitrustalliance.net/csf/hitrust_central_information.php.

About HITRUST

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the CSF, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy and other outreach activities. For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit www.HITRUSTalliance.net.

HITRUST
Health Information Trust Alliance

6136 Frisco Square Blvd.
Suite 327
Frisco, TX 75034

(469) 269-1100
(469) 269-1101
www.HITRUSTalliance.net