Table of Contents

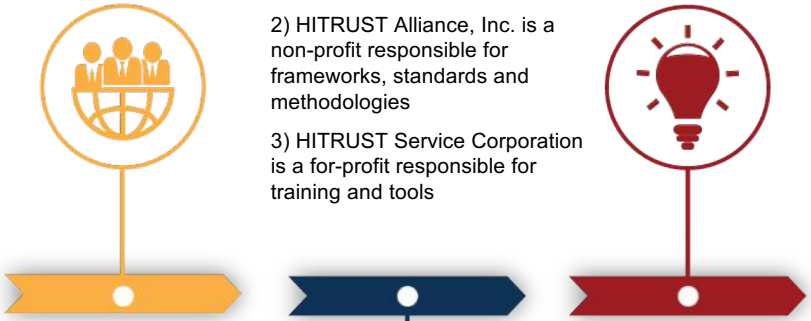
HITRUST 2018 Snapshot

Background

1) Founded in 2007

2) HITRUST Alliance, Inc. is a non-profit responsible for frameworks, standards and methodologies

3) HITRUST Service Corporation is a for-profit responsible for training and tools



Adoption

1) HITRUST CSF is utilized by 81% of US hospitals and health systems and 83% of US health plans

2) HITRUST CSF is the most widely adopted control framework in the healthcare industry, according to a 2018 HIMSS survey

3) GAO Report 2018 Healthcare and Public Health Sector align with HITRUST

3) HITRUST CSF Assurance program is the most widely adopted program for assessing third party risk

Best Known for

1) Developing the HITRUST CSF – 9th major release

- Development guided by a CSF Advisory Council comprised of AHA, AMA, AHIP, AGMA and other security/privacy experts
- Basis for the health and public sector implementation guidance for the NIST Cybersecurity framework, recognized by Department of Homeland Security (link) and Department of Health and Human Services (link)
- Deemed an acceptable controls by the AICPA for a SOC 2 examination
- Identified as an appropriate standard to safeguard Internet of Things (IoT) by NIST (link)

2) Operating the healthcare industry's Information Sharing and Analysis Organization (ISAO)

HITRUST Risk Management Framework

HITRUST was formed to address the growing need and broad desire within the industry for a common framework—a set of common standards and supporting methodologies—that would provide a minimum baseline set of security requirements, tailorable to a specific size and type of organization, which would improve trust as well as mitigate potential liability from breaches of sensitive information. HITRUST believes that improvements in the state of information security and privacy in industry are critical to the broad adoption, utilization and confidence in information systems, information technologies and electronic exchanges of information. The HITRUST risk management framework provides a consistent approach to certification, risk acceptance and shared trust through the HITRUST CSF, CSF Assurance Program, and supporting methodologies and tools such as the HITRUST CSF Assessment Methodology and MyCSF®.

MyCSF is a fully integrated, optimized, and powerful tool that marries the content and methodologies of the HITRUST CSF and CSF Assurance Program. with the technology and capabilities of a governance, risk and compliance (GRC) tool. The user-friendly MyCSF tool 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.

HITRUST Risk Management Framework

HITRUST CSF Assurance Program provides organizations with a single approach for conducting an assessment and reporting against these multiple requirements. Both the HITRUST CSF and CSF Assurance Program are updated at least annually to account for changes in legislation, regulations, standards, guidance and best practices, such as with the 2014 release of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, more commonly known as the NIST Cybersecurity Framework (CsF).

HITRUST CSF Frequently Asked Questions

What assessments are available in MyCSF?

There are three types of assessments available in MyCSF:

- Baseline Assessment – The baseline assessment efficiently measures an organization against a streamlined set of requirements from the 75 controls required for CSF Certification, which are identified and selected based upon risk. A HIPAA scorecard, which reports an organization's compliance with HIPAA requirements only, is also available once a baseline assessment is complete.
- Comprehensive Assessment – The comprehensive assessment efficiently measures an organization against a streamlined set of requirements from all 135 controls of the CSF. Scorecards for any of the other CSF authoritative sources will be available once a comprehensive assessment is complete.
- Detailed Control Assessment – The detailed controls assessment is the most comprehensive measurement of compliance and allows an organization to assess at the most granular level against the prescriptive implementation requirements outlined in each CSF control.

Will an assessment using MyCSF help my organization satisfy the requirements for a risk analysis?

- Yes. A MyCSF Baseline Assessment will cover every implementation specification in the HIPAA Security Rule. However, a MyCSF Comprehensive Assessment will allow an organization to assess controls that support the primary controls mapped from the rule to the HITRUST CSF. Both assessments provide likelihood estimators for probability and impact, which supports the risk calculations needed to determine a risk strategy and prioritization of risk responses.

HITRUST CSF Frequently Asked Questions

Why choose the CSF over other control frameworks like NIST SP 800-53 and ISO/IEC 27001?

- With respect to healthcare industry, the HITRUST CSF was originally built and maintained by the healthcare industry and subsequently, simply better for the healthcare industry. Many of the reasons for choosing the CSF are presented in the following table:

	APPROACH*					
REQUIREMENT	HITRUST (CSF)	ISO (27001)	NIST (800-53)	PCI SSC (DSS)	NIST (CsF)†	HHS (HIPAA)‡
Comprehensive Coverage	YES	YES	YES	YES	YES	PARTIAL
Prescriptive Controls	YES	PARTIAL	YES	YES	NO	NO
Practical Controls	YES	YES	NO	YES	YES	YES
Scalable Implementation	YES	YES	NO	PARTIAL	YES	YES
Transparent Update Processes	YES	PARTIAL	YES	NO	YES	NO
Transparent Evaluation & Scoring Methodology	YES	PARTIAL	PARTIAL	PARTIAL	NO	NO
Consistent Results	YES	PARTIAL	YES	PARTIAL	NO	NO
Accurate Results	YES	PARTIAL	PARTIAL	PARTIAL	NO	NO
Efficient Assessment ("Assess Once, Report Many")	YES	PARTIAL	PARTIAL	NO	PARTIAL	NO
Reliable Results ("Rely-ability")	YES	PARTIAL	PARTIAL	PARTIAL	NO	NO
Certifiable for Implementing Entities	YES	YES	PARTIAL	YES	PARTIAL	NO

HITRUST CSF Frequently Asked Questions

Will an assessment against the CSF help me to achieve implementation of NIST cybersecurity framework?

- Partially, while NIST doesn't provide a certification, HITRUST provides a commensurate alternative. HITRUST has mapped and harmonized the NIST Cybersecurity Framework (CsF) into the HITRUST CSF and updated the HITRUST CSF assurance program to align with the NIST CsF Core Subcategories, in addition to adding an addendum to the HITRUSTCSF Assessment report to provide a scorecard of the HITRUST controls by NIST Subcategory.

How do I get started adopting the CSF framework?

- First, the decision to adopt the CSF should be made at the organizational level, after which organizations should perform an internal gap analysis of existing controls against the target controls in the CSF. This analysis can be done manually or in HITRUST's online GRC-based assessment support tool, MyCSF. Once the information protection posture of the organization is understood, a risk management strategy and implementation timeline can be developed and communicated throughout the organization.

HITRUST CSF Market Differentiation

Adopting and complying with the HITRUST CSF is less expensive and no more complicated than other established risk assessments or certifications.

- By harmonizing relevant standards, regulations and best practices into a single privacy and security framework, the HITRUST CSF is more efficient and certainly no more complicated than other risk assessments or certifications. The design ensures organizations select the requirements relevant to their environment, understand the requirements and expectations for an assessment, and minimize the need to address irrelevant requirements while ensuring a thorough understanding of the expectations during an assessment.

Getting assessed against the HITRUST CSF is less expensive than other assessments.

- The HITRUST Assurance process streamlines the assessment process. As the HITRUST CSF harmonizes many international and US standards, regulations and best practices it also allows organizations to implement controls that satisfy multiple requirements unlike other governance frameworks, this “Assess Once – Report Many” approach allows one assessment to be used to produce a HITRUST CSF Certification, AICPA SOC 2 and NIST Cybersecurity Scorecard or to report against ISO 27001 or NIST 800-53 providing significant efficiencies by eliminating multiple assessments and the related costs and associated resources.

Latest HITRUST News

Latest Release of the HITRUST CSF Integrates GDPR and New York State Cybersecurity Requirements

This latest release is part of HITRUST's commitment to ensure the HITRUST CSF stays relevant to the information risk management, data protection, and regulatory compliance needs of domestic and global organizations through incorporation of new standards and regulations. HITRUST is making the HITRUST CSF – a widely used information privacy and security framework for organizations – more open and comprehensive, so that it can be applied more effectively across a variety of global industries. HITRUST CSF Version 9.1 incorporates both the EU General Data Protection Regulation (GDPR) and New York State Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500). Incorporation of the EU General Data Protection Regulation (GDPR) is part of HITRUST's initiative towards internationalization of the CSF and increased support for global organizational privacy programs.


HITRUST®
For more information on HITRUST and the HITRUST Assessment Xchange, visit www.HITRUSTAlliance.net
To view our latest documents, visit the Content Spotlight