

HITRUST CSF v11.5.0

HITRUST CSF is a certifiable, risk-based cybersecurity and privacy framework for managing regulatory compliance and protecting sensitive data.



What it is

HITRUST CSF v11.5.0 — the HITRUST Common Security Framework — is a certifiable, risk-based cybersecurity and privacy framework that enables organizations to manage regulatory compliance, protect sensitive data, and implement robust information security practices. The framework integrates various standards, regulations, and best practices into a unified approach, making it suitable for organizations that process or handle regulated or sensitive information.

Developed and maintained by HITRUST, the CSF is widely adopted by healthcare organizations, business associates, cloud service providers, and companies seeking to address complex regulatory requirements such as HIPAA, ISO 27001, NIST, and GDPR. It covers key focus areas including security controls, privacy protection, risk management, and ongoing compliance oversight across diverse environments.

At a glance

PUBLISHER HITRUST	TYPE Control Framework	VERSION HITRUST CSF v11.5.0
EFFECTIVE June 2024	DOMAIN Cybersecurity	FAMILY HITRUST
REGION United States	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Certification
IMPLEMENTATION COMPLEXITY Very High		

Source: <https://hitrustalliance.net/hitrust-csf/>

Why it matters

- **Strengthen security governance** Establish clear policies and structured oversight for cybersecurity and privacy across diverse data and operational environments.
- **Enhance regulatory alignment** Align security and privacy controls with multiple standards to streamline compliance obligations and demonstrate fulfillment of requirements.
- **Promote operational resilience** Support business continuity by integrating risk management processes that address threats to information systems and operations.
- **Increase audit readiness** Maintain comprehensive documentation and evidence to simplify audit processes and facilitate consistent third-party validations.

How SmartSuite supports HITRUST CSF v11.5

HITRUST Control Library and Scope

Track HITRUST controls, scope boundaries, and ownership across systems.

Evidence Collection and Audit Trail

Centralize policies, configs, logs, and proof of operation for each requirement.

Assessments and Corrective Actions

Manage assessment activities, findings, remediation, and closure evidence.

Risk and Exception Management

Track exceptions, compensating controls, approvals, and timelines.

Vendor and Third-Party Oversight

Manage BA/vendor requirements, reviews, and monitoring evidence.

Certification Readiness Reporting

Report coverage, open gaps, and readiness across domains and systems.

Common framework mappings

CIS Controls v8.1

HIPAA

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

HITRUST CSF v11.5.0 Overview

Describes HITRUST CSF and its integration with various standards and regulations.
hitrustalliance.net/hitrust-csf

HITRUST CSF Assurance Program

Outlines the process for certification and maintaining compliance with HITRUST CSF.
hitrustalliance.net/assessments-and-certifications

HITRUST CSF Implementation Guidance

Provides guidance on implementing HITRUST CSF controls for effective risk management.
hitrustalliance.net/resources

HITRUST CSF MyCSF Tool

Defines the features of the MyCSF tool for managing and reporting compliance.
hitrustalliance.net/mycsf

Frequently asked questions

What is HITRUST CSF used for?

HITRUST CSF is designed to help organizations manage risk and demonstrate compliance with a range of cybersecurity and privacy regulations. It provides a unified control framework that simplifies meeting requirements of standards such as HIPAA, NIST, ISO 27001, and GDPR. The framework is often used by healthcare entities, business associates, cloud providers, and any organization processing sensitive or regulated data.

Is HITRUST CSF required or certifiable?

HITRUST CSF is a certifiable standard but not a legal requirement. Organizations voluntarily choose to pursue HITRUST certification to demonstrate adherence to recognized security and privacy practices. Certification is achieved through validated assessments conducted by approved HITRUST assessors.

What is the scope of HITRUST CSF and who should consider it?

The framework is broadly applicable to any organization that handles sensitive or regulated information, particularly in healthcare, life sciences, and service provider environments. Scope is determined by identifying systems, business units, or processes handling regulated data and assessing risk accordingly.

What are the core components and artifacts of HITRUST CSF implementation?

Core components include scoped system inventories, risk assessments, the HITRUST control catalog, policies and procedures, and evidence of control operation. Key artifacts generated during implementation include control mapping documentation, maturity assessments, and remediation plans.

How does an organization implement HITRUST CSF?

Implementation involves scoping covered environments, performing risk and gap assessments, selecting and mapping required controls, and developing requisite policies and procedures. Ongoing activities include collecting evidence, addressing gaps, and preparing for HITRUST assessment and certification.

How does HITRUST CSF relate to other compliance frameworks?

HITRUST CSF integrates controls and mappings from multiple frameworks such as HIPAA, NIST SP 800-53, ISO 27001, and GDPR, offering organizations a harmonized approach to address diverse regulatory requirements. This integration streamlines compliance by reducing the need for maintaining separate controls for each standard.

What are the ongoing requirements for maintaining HITRUST CSF certification?

Organizations must conduct regular self-assessments or validated assessments, remediate identified deficiencies, maintain up-to-date documentation, and provide continuous evidence of control effectiveness. Annual or biennial recertification is required to maintain certified status.

How would SmartSuite support HITRUST CSF v11.5.0?

SmartSuite enables organizations to operationalize HITRUST CSF by importing the control library, maintaining risk registers, and mapping controls. It streamlines evidence collection, compliance tracking, and remediation workflows. SmartSuite also facilitates audit readiness with dashboards, reporting tools, and the ability to assign tasks and demonstrate real-time control status during assessments.

License included / downloadable: No HITRUST CSF is published by the HITRUST Alliance. Access to the full framework documentation and certification program typically requires licensing or participation in the HITRUST program. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/hitrust-csf-v11-5-0-hitrust-common-security-framework