360ADVANCED

YOUR GUIDE TO

# YOUR GUIDE TO HITRUST® CSF CERTIFICATION & ASSESSMENT

INFO@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

# Table of Contents

# Introduction & Purpose

The purpose of this guide is to provide organizations with a clear, concise overview of the HITRUST CSF and the associated certification process. Specifically designed for businesses navigating the complex landscape of information security and regulatory compliance, this document clarifies how HITRUST certification helps effectively manage information risk and compliance obligations, particularly within the healthcare industry and other highly regulated sectors.

HITRUST CSF certification signifies to clients, partners, and regulatory bodies that an organization has implemented robust, comprehensive security and privacy controls. However, this guide is strictly educational; it does not promote or endorse any particular service provider, assessor, or commercial offering.

# What Is HITRUST & the HITRUST CSF?

The Health Information Trust Alliance (HITRUST), established in 2007, created the HITRUST CSF to streamline and standardize the compliance process across multiple regulations and standards. The CSF is a comprehensive security framework that integrates requirements from more than 60 major regulations, standards, and frameworks, including HIPAA, ISO/IEC 27001/27002, NIST SP 800-53, GDPR, and PCI-DSS, into a unified approach.

This framework helps organizations efficiently address security, privacy, and regulatory compliance through a single assessment process. HITRUST regularly updates the CSF to reflect evolving cyber threats, regulatory changes, and emerging security needs, such as those introduced by artificial intelligence and cloud computing environments.

Organizations achieving HITRUST certification can demonstrate their commitment to protecting sensitive data through verified compliance with industry-recognized best practices. The HITRUST CSF allows entities to validate security and privacy controls comprehensively, effectively meeting the demands of customers, stakeholders, and regulatory authorities.

# Assessment & Certification Types

HITRUST offers several assessment types to cater to varying organizational needs and risk profiles:

### HITRUST Essentials (e1)

An entry-level assessment focusing on fundamental cybersecurity hygiene practices, suitable for organizations new to formal compliance processes. Certification lasts for one year.

### HITRUST Implemented (i1)

Designed for organizations seeking to implement best practices with broader coverage than the Essentials assessment. Certification also lasts for one year.

### HITRUST Risk-based (r2)

A comprehensive, risk-adaptive evaluation suitable for organizations that require a deep and thorough review of security and privacy controls. This certification is valid for two years.

### HITRUST AI Security Assessment and Certification

The AI Security Assessment is designed to provide AI platform and service providers with relevant, prescriptive, practical security controls and methodology to confidently adopt and secure AI technologies.  It supports shared responsibility inheritance and when paired with an e1, i1, or r2, enables organizations to address multiple compliance needs within a streamlined solution.

Organizations may initially select lighter self-assessments or proceed directly to certified validated assessments based on their resources, maturity, and specific risk management requirements.

## Why Consider Using HITRUST CSF?

The HITRUST CSF framework harmonizes numerous authoritative sources into a unified, cohesive control framework, streamlining compliance management. Since it's globally recognized, there has been significant adoption, with nearly 30,000 organizations downloading the framework within the past five years. The CSF utilizes artificial intelligence to integrate new regulatory and security requirements rapidly and accurately, and it also provides dedicated assessment options specifically designed for AI systems. Regular updates ensure the framework remains current with evolving regulatory landscapes and emerging threats.

# Phases of the HITRUST Process

The certification process typically unfolds across several key phases:

01

### Readiness Assessment

Organizations utilize HITRUST's MyCSF tool to perform a gap analysis, identifying areas requiring improvement prior to formal assessment.

02

### Remediation Planning

Based on findings from the readiness assessment, organizations develop and execute corrective action plans to address identified gaps.

03

### Validated Assessment

Conducted by an authorized external assessor, this phase involves detailed reviews of documentation, interviews with key personnel, and thorough testing of implemented controls.

04

### HITRUST Quality Assurance Review

After the validated assessment, HITRUST conducts a rigorous quality assurance review of the assessor's findings, typically requiring four to eight weeks before issuing the final certification report.

The total duration for initial certification can vary significantly but often extends up to 12 months, depending on an organization's scope, size, and existing maturity of security and privacy practices.

# Key Roles & Stakeholders

Successfully navigating the HITRUST CSF assessment requires clearly defined roles and responsibilities within your organization, along with collaboration from external stakeholders.

**Primary roles include:**

- **Information Security Officer (ISO)/Chief Information Security Officer (CISO):** Oversees the entire security strategy, aligns compliance objectives with organizational goals, and reports to executive management.
- **Compliance and Privacy Officers:** Focus on regulatory adherence and privacy protection efforts, aligning internal policies with HITRUST certification requirements.
- **IT and Security Operations Teams:** Implement and manage cybersecurity controls, providing required documentation and addressing gaps identified in assessments.
- **Risk Management Teams:** Identify, assess, and mitigate risks, aligning the HITRUST certification process with overall organizational risk management.
- **Executive Leadership:** Ensures organizational support and strategic oversight, establishing a compliance-focused culture.
- **External Authorized HITRUST Assessors:** Independent third-party professionals conducting validation through testing, documentation reviews, and assessments.
- **HITRUST Alliance Quality Assurance (QA) Team:** Conducts final reviews of assessments, ensuring integrity and quality before certification issuance.

Clear communication, coordination, and accountability among these stakeholders are critical for achieving and maintaining HITRUST certification.

# Benefits & Limitations

HITRUST CSF certification offers proven economic advantages to organizations by significantly improving operational efficiency, reducing risk, and facilitating business growth. According to a recent analysis by the Enterprise Strategy Group (ESG), companies adopting HITRUST certification realized measurable financial benefits, including streamlined compliance management, reduced preparation time for audits, and enhanced market competitiveness. ESG found that organizations utilizing HITRUST achieved an average return on investment of 464%, underscoring the framework's value in proactively managing cybersecurity risk and regulatory compliance.

## Benefits

- **Comprehensive Framework:** Integrates multiple regulatory requirements into a unified approach.
- **Regulatory Compliance:** Demonstrates compliance with numerous standards simultaneously, reducing redundant assessments.
- **Enhanced Security Posture:** Indicates mature security programs, enhancing trust among stakeholders.
- **Market Differentiation:** Provides competitive advantage through rigorous cybersecurity practices.
- **Operational Efficiency:** Utilizes HITRUST's MyCSF tool for streamlined assessments and continuous monitoring.

## Limitations

- **Cost and Resource Intensity:** Requires significant financial investment and dedicated resources, particularly for first-time certifications.
- **Complexity for Small Organizations:** Comprehensive assessments may be challenging for smaller organizations with limited resources.
- **Certification Scope Constraints:** Changes in organizational scope require reassessment and potential additional costs.
- **Rapidly Evolving Regulatory Landscape:** Frequent updates necessitate regular adaptation to maintain certification.

Understanding these factors will help your organization effectively navigate the HITRUST certification process.

# Maintaining Certification & Recertification

Maintaining HITRUST certification requires ongoing monitoring, management of security and privacy controls, and periodic reassessments:

### Continuous Monitoring

Organizations must continuously monitor and manage their security and privacy controls to maintain compliance.

### Interim Assessments

Depending on the assessment type, interim assessments or annual reviews may be required.

### Recertification

Organizations must undergo a full recertification assessment before their certification expires. This involves a new validated assessment and HITRUST QA review.

### Updates and Adaptation

Organizations should stay informed of updates to the HITRUST framework and adapt their controls and processes accordingly to maintain certification.

# Further Resources / References

- HITRUST Alliance Official Website
- HITRUST CSF Documentation
- MyCSF User Guide
- HITRUST Certification FAQs