HITRUST Compliance

Advisory & Certification Readiness Support

What is HITRUST?

The Health Information Trust Alliance (HITRUST) provides a comprehensive, risk-based, certifiable framework designed to help organizations protect sensitive data and align with multiple regulatory requirements. HITRUST introduced and maintains the Common Security Framework (CSF), which standardizes compliance with regulations such as HIPAA and aligns them with other national and international security standards.

By integrating requirements from numerous regulations and best practices, HITRUST CSF enables organizations to complete a single, comprehensive assessment that supports compliance across multiple initiatives—streamlining audits, reducing redundancy, and strengthening overall security posture.

Why Your Company Should Pursue HITRUST Certification

Achieving HITRUST certification signals a strong commitment to data protection and regulatory compliance. It demonstrates that your organization meets rigorous security standards and follows industry-recognized best practices. Key Benefits:

- Demonstrates compliance with frameworks such as HIPAA, NIST, and ISO
- Enhances credibility with customers, partners, and stakeholders
- Streamlines vendor due diligence and third-party risk assessments
- Structured, scalable information security programs

HITRUST vs. HIPAA

HIPAA is a federal regulation that mandates the protection of personal health information but does not prescribe specific security controls or offer a certification process. HITRUST, on the other hand, provides a certifiable framework that maps directly to HIPAA requirements while also incorporating additional regulatory and security standards.

Unlike HIPAA, HITRUST allows organizations to undergo third-party validated assessments and earn formal certification that demonstrates compliance and cybersecurity readiness.

Degrees of HITRUST Assurance

HITRUST CSF offers three levels of assessment, varying in rigor, cost, and effort:

Self-Assessment

An internal evaluation used to measure cybersecurity and compliance posture. While HITRUST provides a Self-Assessment Report, it does not confer certification or third-party assurance.

Validated Assessment

A HITRUST-approved third-party assessor verifies evidence and conducts required testing. HITRUST reviews the validated results and issues a Validated Report.

Certified Assessment

Builds on the Validated Assessment. HITRUST performs an additional quality assurance review and formally certifies the organization, issuing a HITRUST CSF Certified Report.

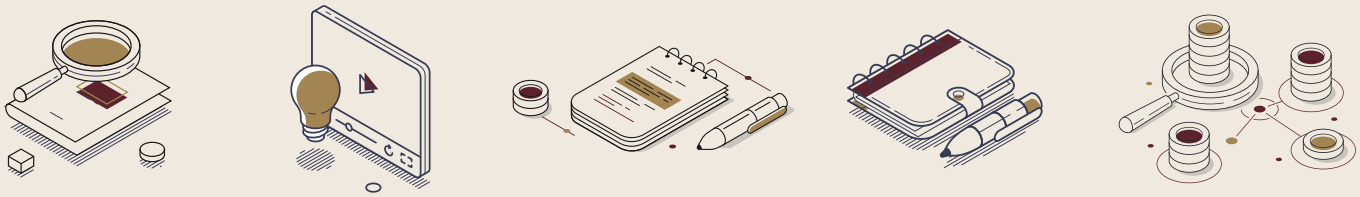
HITRUST CSF Control Categories

HITRUST CSF is organized into 14 control categories that address administrative, technical, and physical security requirements:

- Information Security Management Program
- Access Control
- Human Resources Security
- Risk Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Privacy Practices

The RSI Security 5-Step HITRUST Process

The HITRUST CSF certification lifecycle follows a two-year cycle.



Gap Assessment

A comprehensive evaluation of your organization's cybersecurity environment, policies, procedures, and documentation to identify gaps against HITRUST CSF requirements and determine readiness.

CSF Implementation

Guided implementation of the HITRUST CSF control requirements based on your assessed gaps, including policy development, technical controls, and process alignment.

Validation Readiness

Preparation for third-party validation, including evidence collection, remediation support, and coordination with an authorized HITRUST CSF assessor.

Certification Review

Submission support and coordination through HITRUST's quality assurance review process, which evaluates validated documentation before certification is granted.

Ongoing Management

Support for maintaining compliance throughout the two-year certification cycle, including monitoring updates to the HITRUST CSF, evolving threats, and organizational changes.

RSI

Ready to Take the Next Step?

RSI Security supports organizations at every stage of the HITRUST CSF journey—from readiness and implementation to validation coordination and ongoing compliance management. With over a decade of cybersecurity and compliance experience, our team brings practical, hands-on expertise across complex regulatory environments.

858.999.3030 | info@rsisecurity.com | rsisecurity.com