NETWORK INTELLIGENCE
The Digital Security Company

HITRUST Certification
Implementation Guide

A Comprehensive Approach to Achieving HITRUST Certification

This HITRUST Implementation Guide will walk you through the necessary prerequisites and steps to meet compliance head-on and connect the dots between HITRUST CSF controls and the local regulations so that you can protect data smartly and effectively.

Know About HITRUST

HITRUST Certification is a comprehensive security and compliance framework that incorporates more than 40 regulatory standards, including HIPAA, SOC 2, NIST, and ISO 27001. HITRUST compliance offers a scalable and unified approach to meeting various regulatory requirements.

How has HITRUST Contributed?

HITRUST Certification saved 99.36% of HITRUST-certified environments from breaches in 2022 and 2023
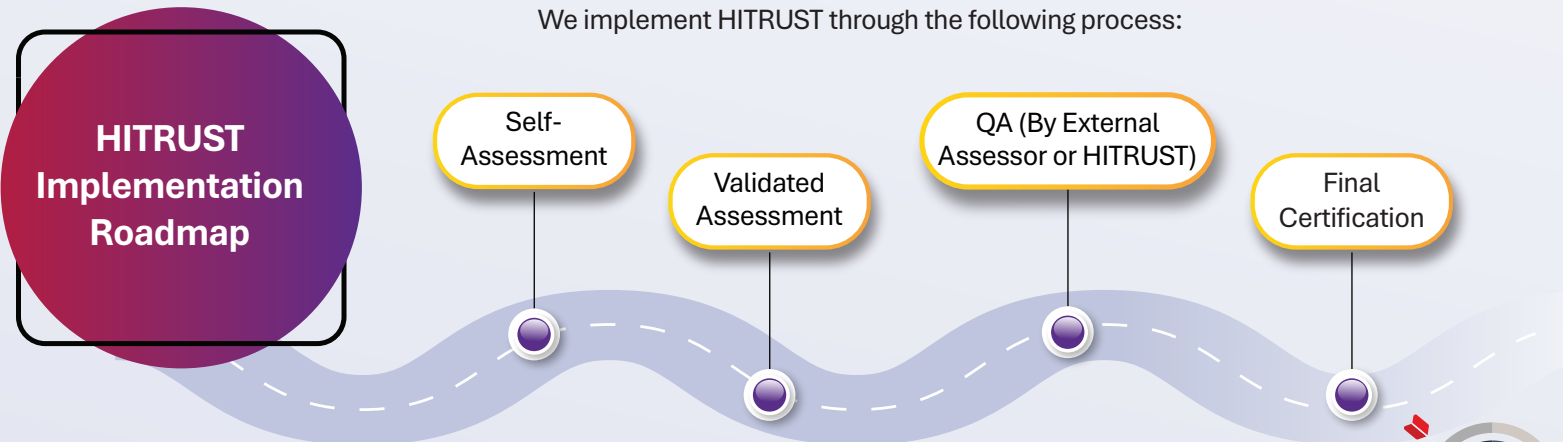
Source: HITRUST Trust Report

Why Should You Take HITRUST Compliance Certification?

Achieving HITRUST compliance certification offers numerous benefits that enhance your organization's security posture:

1. Makes security and compliance simpler
2. Reduced need for multiple audits
3. Strengthens security and privacy controls
4. Approved and assured standard for certifications
5. Builds credibility with customers and partners
6. Saves audit costs and potential losses

We implement HITRUST through the following process:

HITRUST Implementation Roadmap

- Self-Assessment
- Validated Assessment
- QA (By External Assessor or HITRUST)
- Final Certification

A. HITRUST ASSESSMENT

Goal: Evaluation of how well your organization follows the HITRUST CSF and to check your organization's compliance and risk management status.

Types of Assessment

The i1 and r2 assessments are performed in validated assessments to achieve certification.

e1 (Essential), Valid for 1 Year

Controls: 44 controls

Timeline: Approx 3 months

Focus:
- To ensure fundamental cybersecurity hygiene is implemented
- Concentrates on the most vital cybersecurity controls
- Basic evaluation focusing on fundamental data protection and cybersecurity procedures.

Applicable To:
Small organizations new to HITRUST and want a simpler entry point into security and compliance.

Level of Assurance Conveyed: Low

i1 (Implemented), Valid for 1 Year

Controls: 182 controls

Timeline: 6 to 12 months

Focus:
- In the direction of earning an r2 certification
- Evaluation of foundational controls
- Assessment of policy, procedures, implementation, measurement, and management

Applicable To:
Organizations with strong information security programs and those prepared to showcase best practices in security.

Level of Assurance Conveyed: Moderate, relative to r2 certification

r2 (Risk-based Assessment), Valid for 2 Years (Interim assessment is required)

Controls: 200+ controls

Timeline: 18 to 24 months

Focus:
- To evaluate maturity across domain and control customization based on risk analysis.
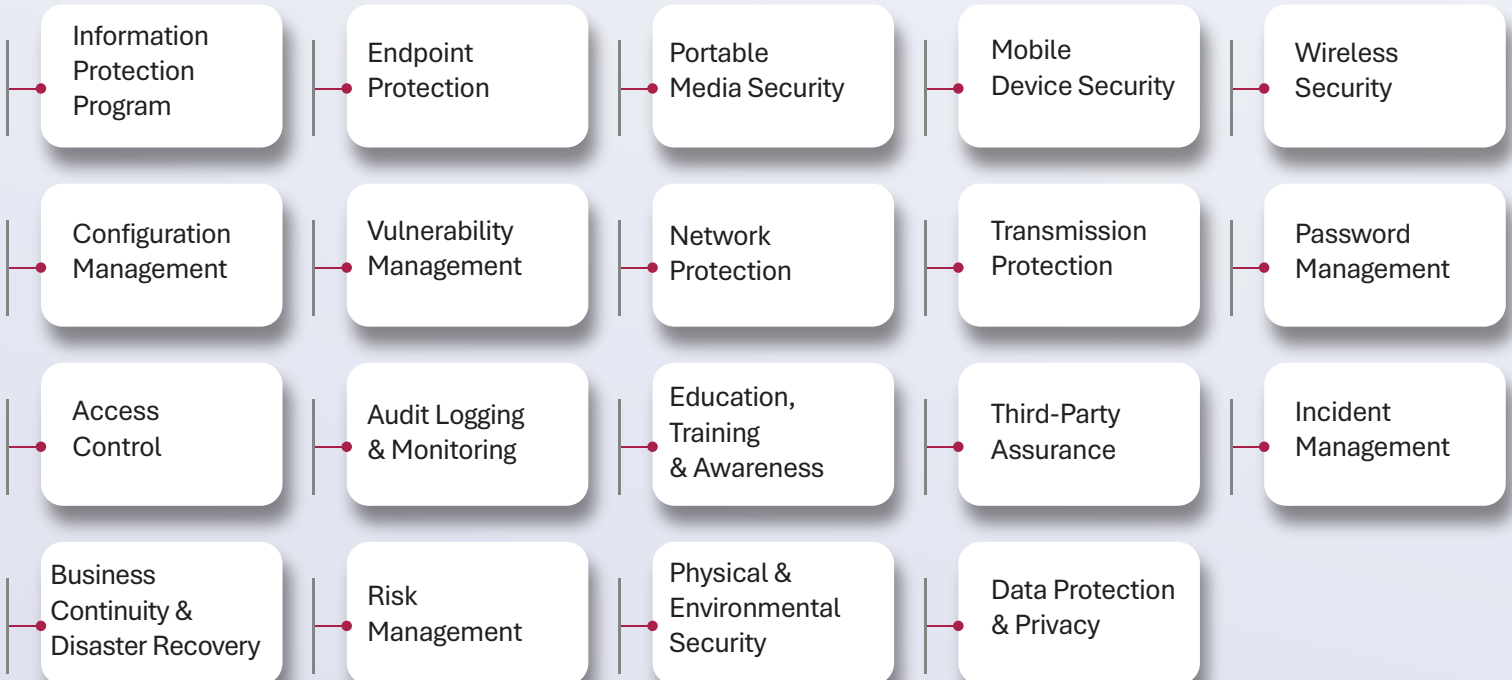- Third-party risk management, asset management, data integrity, etc.

Applicable To:
Established organizations handling large volumes of sensitive data or PHI, requiring high-level assurance.

Level of Assurance: Highest

HITRUST Assessment Domains

Requirement statements are distributed across 19 domains, which emphasize precision in targeting data protection.

Information Protection Program	Endpoint Protection	Portable Media Security	Mobile Device Security	Wireless Security
Configuration Management	Vulnerability Management	Network Protection	Transmission Protection	Password Management
Access Control	Audit Logging & Monitoring	Education, Training & Awareness	Third-Party Assurance	Incident Management
Business Continuity & Disaster Recovery	Risk Management	Physical & Environmental Security	Data Protection & Privacy	

Control Categories

The CSF contains 14 control categories, consisting of:

49 control objectives and

156 control specifications

The CSF control categories, accompanied by their respective number of control objectives and control specifications for each category are:

Information Security Management Program (1, 1)

Access Control (7, 25)

Human Resources Security (4, 9)

Risk Management (1, 4)

Security Policy (1, 2)

Organization of Information Security (2, 11)

Compliance (3, 10)

Asset Management (2, 5)

Physical and Environmental Security (2, 13)

Communications and Operations Management (10, 32)

Information Systems Acquisition, Development, and Maintenance (6, 13)

Information Security Incident Management (2, 5)

Business Continuity Management (1, 5)

Privacy Practices (7, 21)

B. HITRUST CERTIFICATION

Goals: To standardize compliance across multiple regulatory frameworks.

Our Approach to HITRUST Certification

Step 1: Define Scope

- Organizations opt to collaborate with a third-party assessor or an internal subject matter expert to define the scope and select the appropriate HITRUST assessment to undergo.

Step 2: Obtain Access to MyCSF Portal

- The organization being assessed contacts HITRUST to get access to the MyCSF portal.
- After receiving access, the organization should create its assessment object and engage an approved third-party assessor firm.

Step 3: Complete a Readiness Assessment/Gap-Assessment

- The assessor performs appropriate tests to understand the organization's environment and flow of data between systems.
- The assessor does gap assessment, documents them, and ranks gaps in your organization by risk level, allowing you to remediate any gaps before the validated assessment.

- During the validated assessment phase (e1, i1, or r2), assessors will review and validate client scores.
- The final assessment is submitted to HITRUST for approval.
- HITRUST either approves or denies your organization's certification.
- HITRUST Quality Assurance (QA) stage, prior to certification issuance, may span from four to ten weeks based on the assessment and assessors' responsiveness.

Step 5: Interim Assessment Testing

- If certification is obtained as part of the r2 Assessment, an interim assessment is required to be conducted at the one-year mark to maintain certification.
- Note: Interim assessment is not required if certification was obtained via the e1 or i1 Assessment

Find out how we make HITRUST certification effortless!

Compliances and Accreditations at Core

Our knowledge of regulatory frameworks enhances our HITRUST certification processes, allowing us to provide accurate, efficient, and trustworthy compliance solutions for our clients.

Our Accreditations

HITRUST Authorized External Assessor

CSA CLOUD SECURITY ALLIANCE Trusted Cloud Consultant

CREST

PCi DSS COMPLIANT

Swift CSP

About Network Intelligence

- 24+ Years
- 550+ team members
- Presence in the US, Europe, Middle East, Southeast Asia, and India
- Domain Expertise: Financial Services, Healthcare, Retail, Ecommerce, Utilities, and Others

We Are Your Trusted Partner for HITRUST Certification

Network Intelligence is your go-to partner for smooth, fast, and reliable certification and HITRUST services. Let us remove the complexities of compliance so you can focus on growing your business.

Contact Us

✉ https://networkintelligence.ai/

🌐 contact@networkintelligence.ai

NETWORK INTELLIGENCE
The Digital Security Company

HITRUST®
Authorized External Assessor