# HITRUST Overview

## Summary

The **HITRUST Common Security Framework (CSF)** is a certifiable, risk-based framework developed by the **HITRUST Alliance** to help organizations, primarily in healthcare, manage security and privacy risks while complying with regulations like **HIPAA**, **ISO 27001**, **NIST**, and others. Launched in 2007 and regularly updated (v11.3 in 2025), HITRUST CSF integrates multiple standards into a single, scalable framework for protecting sensitive data, such as protected health information (PHI). It offers a structured approach with 14 control categories, customizable controls, and three implementation levels (1–3) based on risk. Certification is voluntary but widely adopted in healthcare for demonstrating compliance to regulators, partners, and customers. Non-compliance with HITRUST (if required by contracts) can lead to loss of business, reputational damage, or regulatory scrutiny. As of October 2025, HITRUST emphasizes cloud security, AI risk management, and third-party assurance.

## Key Requirements

HITRUST CSF organizes **135 controls** (in v11.3) across **14 control categories**, mapped to regulations like HIPAA, NIST 800-53, and GDPR. Controls are tailored to organizational risk, size, and complexity via three implementation levels (Level 1: basic, Level 2: moderate, Level 3: advanced). Key requirements include:

1. **Security Management**:
    - Establish a security program with policies, risk assessments, and governance.
    - Appoint a security officer to oversee compliance.
2. **Access Control**:
    - Implement role-based access, multi-factor authentication (MFA), and session controls.
    - Restrict access to authorized users/devices handling sensitive data.
3. **Human Resources Security**:
    - Conduct background checks and security training for employees.
    - Enforce policies for onboarding, termination, and role changes.
4. **Risk Management**:
    - Perform annual risk assessments to identify threats (e.g., cyberattacks, insider threats).
    - Develop risk treatment plans and monitor mitigation progress.
5. **Information Security Incident Management**:
    - Create and test incident response plans for data breaches.
    - Report significant incidents (e.g., PHI breaches) per HIPAA or contract requirements.
6. **Business Continuity and Disaster Recovery**:
    - Develop and test business continuity plans (BCPs) for system disruptions.
    - Maintain secure backups and recovery procedures.
7. **Physical and Environmental Security**:

    - Secure facilities with locks, badges, and surveillance for systems storing sensitive data.
    - Protect against environmental threats (e.g., power outages, floods).
8. **Endpoint Protection**:
    - Deploy anti-malware, endpoint detection and response (EDR), and encryption (e.g., AES-256).
    - Monitor endpoints for unauthorized activity.
9. **Network Protection**:
    - Use firewalls, intrusion detection/prevention systems (IDPS), and encryption (e.g., TLS 1.3).
    - Implement zero-trust architecture for network security.
10. **Third-Party Management**:
    - Assess and monitor vendors handling sensitive data via contracts and audits.
    - Ensure vendors comply with HITRUST or equivalent standards.
11. **Data Protection and Privacy**:
    - Protect PHI/PII with encryption, data minimization, and access controls.
    - Provide privacy notices and honor data subject rights (aligned with HIPAA/GDPR).

**Certification Process**:

- **Self-Assessment**: Conduct a preliminary assessment using HITRUST CSF tools.
- **Validated Assessment**: Engage a HITRUST Authorized External Assessor for a formal audit (1–2 years validity).
- **Remediation**: Address gaps via corrective action plans (CAPs).
- **Continuous Monitoring**: Maintain compliance with annual reviews and interim assessments.
- **MyCSF Tool**: Use HITRUST's online platform for assessment and reporting.

**2025 Context**: HITRUST CSF v11.3 enhances AI governance, cloud security, and supply chain risk management, aligning with NIST CSF 2.0 and HIPAA's telehealth focus.

**Who Is Affected**

- **Organizations**:
    - Primarily healthcare entities (e.g., hospitals, insurers, providers, clearinghouses) handling PHI.
    - Non-healthcare organizations (e.g., IT vendors, cloud providers) processing sensitive data for healthcare clients.
    - Any organization seeking HITRUST certification for regulatory compliance or competitive advantage.
- **Business Associates**:
    - Third-party vendors (e.g., EHR providers, cloud services) handling PHI under HIPAA Business Associate Agreements (BAAs).
- **Employees**:
    - IT, security, and compliance staff implementing HITRUST controls.

    - All staff handling PHI require training and adherence to policies.
- **Customers/Clients**:
    - Patients or businesses relying on certified organizations for secure data handling.
- **Regulators and Partners**:
    - HHS OCR (for HIPAA alignment), though HITRUST is not directly enforced.
    - Partners (e.g., insurers, hospitals) often require HITRUST certification in contracts.
- **Impact of Non-Compliance**:
    - Loss of contracts or partnerships requiring HITRUST certification.
    - Regulatory scrutiny (e.g., HIPAA fines up to $1.9M per violation type, 2025). (Clarification: This is the annual cap per violation category, not per individual violation.)
    - Reputational damage and loss of customer trust.

**Informational Resources**

- **HITRUST Alliance Website**: hitrustalliance.net (overview, CSF details, certification process).
- **HITRUST CSF Framework**: hitrustalliance.net/csf (access to v11.3 framework, requires license or free trial).
- **MyCSF Portal**: hitrustalliance.net/mycsf (assessment tool, subscription-based).
- **Training and Tools**:
    - HITRUST Academy: hitrustalliance.net/training (certification training, e.g., CCSFP certification).
    - HITRUST CSF Assessor List: hitrustalliance.net/assessors (find authorized auditors).
    - NIST HIPAA Security Rule Toolkit: csrc.nist.gov/projects/security-content-automation-protocol/hipaa (complements HITRUST with HIPAA mappings).
- **Industry Resources**:
    - “HITRUST CSF Guide” (free PDFs from vendors like Coalfire, A-LIGN).
    - Healthcare Information and Management Systems Society (HIMSS): himss.org (HITRUST/HIPAA resources).
    - AHIMA Resources: ahima.org (compliance guides for healthcare).
- **Community Support**:
    - HITRUST Community Events: hitrustalliance.net/events (webinars, forums).
    - Healthcare Compliance Association (HCCA): hcca-info.org (HITRUST/HIPAA discussions).
    - ISACA Cybersecurity Community: isaca.org (HITRUST implementation advice).