Guide to HITRUST CSF Certification

A unified cybersecurity and compliance risk management program

What is HITRUST Common Security Framework (CSF)?

HITRUST Common Security Framework (CSF) is a robust security and privacy risk framework

- Built upon other existing, industry-accepted information security and privacy standards and regulations
- Provides a robust set of prescriptive control requirements to support establishment and maintenance of security, privacy, and compliance goals

Key benefits of adopting the HITRUST CSF Framework:

- **Certifiable** – provides third party assurance to organizations' security and privacy practices
- **Scalable** – allowing for innovation while securing data in accordance with organization type, size, and operational and regulatory complexity
- **Comprehensive** - leverages existing globally recognized standards and reduces unnecessary redundancy
- **Prescriptive** - ensure clarity of requirements and scope and eliminate ambiguity in expectation and maturity levels
- **Evolving** – regularly maintained by HITRUST organization to address changes in regulations and standards

Subset of standards and regulations incorporated in the HITRUST CSF

Regulatory Requirements

- HIPAA and HITECH
- FISMA
- FedRAMP
- FTC Red Flags Rule
- SCIDSA

Information Security Frameworks

- PCI-DSS
- NIST
- ISO 27000

Implementation Standards

- NIST 800 Series
- PCI DSS
- ISO 27000 Series
- ITIL
- SANS
- COBIT

Privacy Frameworks

- EU GDPR
- CCPA
- Massachusetts Data Protection Act
- Singapore Personal Data Protection Act

HITRUST CSF Assessment – Level of Assurance

Low

Basic, Current-State (bC) Assessment

“good hygiene” assessment and offers higher reliability than self-assessments

- Not certifiable
- 71 Static controls with no tailoring
- Verified using HITRUST Assurance Intelligence Engine™
- Focus: NISTIR 7621: *Small Business Information Security Fundamentals*

Moderate

1-year (i1) Validated Assessment

“best practices” assessment for where a baseline risk assessment is needed

- Certifiable, 1 Year
- 219 Static controls with no tailoring
- Focus: NIST SP 800-171, HIPAA Security Rule

High

2-year (r2) Validated Assessment

Industry standard assessment that is a risk-based and tailorable

- Certifiable, 2 Year
- 2000+ controls based on Tailoring (360 average in scope of assessments)
- Tailor based on unique organizational risk: NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, AICPA TSC, PCI DSS, GDPR, and 37 others

What is included in a HITRUST CSF assessment?

HITRUST CSF allows for significant tailoring based the following scoping factors. Factors that increase risk to the security and privacy of data may increase the control requirements to be included in the assessment.

- General (e.g. type, size, location)
- Organizational (e.g. number of records held)
- Geographical (e.g., state, multi-state, international)
- System Factors (e.g., connection to the internet, use of mobile devices, third party access)
- Regulatory Factors (e.g., PCI, HIPAA, GDPR, CCPA)

Control requirements are mapped across 19 HITRUST CSF assessment domains based on common IT processes. These 19 domains are used as a basis for scoring the assessment.

01	**Information Protection Program**
02	Endpoint Protection
03	Portable Media Security
04	Mobile Device Security
05	Wireless Security
06	Configuration Management
07	Vulnerability Management
08	Network Protection
09	Transmission Protection
10	Password Management
11	Access Control
12	Audit Logging & Monitoring
13	Education, Training & Awareness
14	Third-Party Assurance
15	Incident Management
16	Business Continuity & Disaster Recovery
17	Risk Management
18	Physical & Environmental Security
19	Data Protection & Privacy

HITRUST - How are requirements scored?

1	2	3	4	5
Policy	**Procedure**	**Implemented**	**Measured**	**Managed**
What are the established high-level requirements?	What are the steps necessary to perform the requirements?	How are the requirements operated?	Does the organization ensure it is working properly?	Are the activities well integrated?
Policies or standards contain established and finite requirements to guide present and future decisions	Procedures address how to perform each requirement at a sufficient level of detail	Requirements are implemented and operating as intended and designed, across applicable systems and organizational units	Control requirements are tested and measured (metrics) over time to determine whether they continue to remain effective	Metrics are managed via a defined management process that includes root cause analysis and corrective action based on the results
15 pts.	20 pts.	40 pts.	10 pts.	15 pts.

Required for certification

HITRUST - How are requirements scored?

Each control requirement is evaluated for ***coverage*** (i.e., % of elements of the control requirement addressed) and ***strength*** (i.e., % of criteria or scope elements addressed) and assigned an implementation level estimate as follows:

Maturity Level Scoring	Non-Compliant (NC)	Somewhat Compliant (SC)	Partially Compliant (PC)	Mostly Compliant (MC)	Fully Compliant (FC)
Implementation Level Estimate	**0-10% - Very few** if any of the control requirements are implemented for the maturity level assessed	**11-32% - Some** of the control requirements are implemented for the maturity level assessed	**33-65% - About half** of the control requirements are implemented for the maturity level assessed	**66-89% - Many** of the control requirements are implemented for the maturity level assessed	**90-100% - Most if not all** of the control requirements are implemented for the maturity level assessed
Maturity Estimate	0%	25%	50%	75%	100%

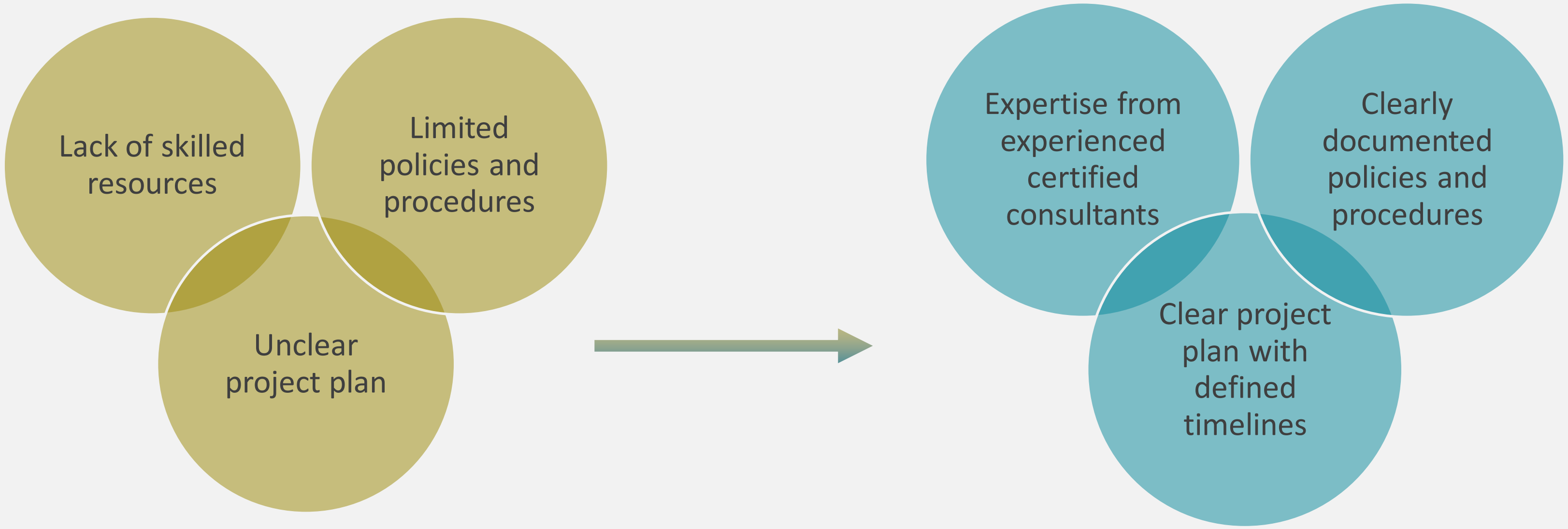
Maturity scoring = **maturity level points (15 pts, 20 pts, 40 pts, 10 pts, and 15 pts) x maturity estimate (0%, 25%, 50%, 75%, and 100%).** A score of **3+ (> 71)** is considered the standard for a fully implemented control.

	Maturity Level Scoring/ Score to Rating Conversion														
Cut-off Score	0	9.99	18.99	26.99	35.99	44.99	52.99	61.99	70.99	78.99	82.99	86.99	89.99	93.99	97.99
Maturity Level	1-	1	1+	2-	2	2+	3-	3	3+	4-	4	4+	5-	5	5+

Additional Considerations:

- Each domain MUST score a 3 to meet certification requirements
- Any control requirement that scores less than a 3+ will require a Corrective Action Plan (CAP)
- Management may choose to accept the risk of not addressing a requirement, but only for a control requirement with a score of 3

Customer Success Story


Lack of skilled resources
Limited policies and procedures
Unclear project plan
Expertise from experienced certified consultants
Clearly documented policies and procedures
Clear project plan with defined timelines

Customer Objective

- SaaS provider looking to complete in the healthcare space
- Scalable long-term compliance strategies
- Key considerations: **Expertise, cost, and time**

Secliance Solution

- HITRUST Certification in 6 months
- Process documentation with step-by-step descriptions of how to execute the control requirements
- Sustainable continuous monitoring program

Secliance Readiness Services

Comprehensive service to achieve and maintain HITRUST Certification

Strategize

- Physical and Logical Boundary
- Team Workshops
- HITRUST Gap Assessment

Implement

- Program and Playbook Development
  - Policies and Procedures
  - Incident Response Program
  - Risk Management Program
  - Information Security Management Program
  - Insider Threat Management
  - Security Awareness and Training
  - Business Continuity and Disaster Recovery
- Technical Remediation Support

Transform

- External Assessment Support
- Continuous Monitoring Program

Steps to HITRUST CSF and obtaining certification

HITRUST
CSF Certified
1
2
3
4

Establish objectives and scope

- Why and what systems?
- What scoping factors are applicable?
- Who are the project sponsors?
- Which control requirements are in scope?

Readiness assessment

- What is the status of policies, procedures, and implementation of applicable control requirements?
- Are there missing elements?

Gap Remediation

- Create or update missing policies and procedures to ensure all elements are addressed as necessary
- Implement missing controls
- Develop and track corrective action plans for identified gaps

Validation by Approved Assessor

- Appoint a point of contact to work with the assessor
- Assessor will review documentation, interview personnel, and evaluate controls via observation or sample testing

HITRUST CSF certification timeline

SCOPING AND READINESS

Organization will:

- Define scope of the assessment
- Gather necessary information (e.g., policies, procedures, records, logs, vulnerability assessment reports, risk assessment reports)

0 – 12 months

Dependent on initial readiness and amount of remediation needed to fully implement the requirements

Tick

EXTERNAL ASSESSMENT

Assessor will:

- Examine documentation (Policies, standards, guidelines, procedures, records, etc.)
- Interview key stakeholders
- Test implementation of controls, as applicable

90 days maximum

Controls to be assessed have to be in place a minimum of 90 days prior to assessor testing

Tock

SUBMISSION TO HITRUST

Assessor will:

- Submit the completed baseline questionnaire, along with description of scope, overview of the organization’s security program, testing performed, and corrective action plans to **HITRUST**
- Coordinate the review process between **HITRUST** and **Organization**

5 days

Dependent on successful check-in of the sybmission in MyCSF

Tick

HITRUST REVIEW

HITRUST will:

- Review the assessment report and associated artifacts, as applicable
- Provide a draft assessment report to organization
- Issue a final report to the **organization**

8 weeks

Following acceptance or successful check-in of the submission in MyCSF

Tock

ONGOING MAINTENANCE

Organization will:

- Maintain effectiveness of the control processes
- Complete an interim assessment no later than **1 year from date of validated report date/certification**
- Re-certify every **2 years** from HITRUST CSF Validated Report date

Ongoing

Interim testing can being 120 days before the 1-year anniversary

Tick

Secliance

Strategize. Implement. Transform.

Thank You

Feel free to contact us:

☎ +1 800 674 8433

✉ support@secliance.com

For more information visit:
www.secliance.com

Contact me directly at:

Stella Bridges, CCSFP, CISSP, GSTRT, CPA, CISA
Managing Principal
stella.bridges@secliance.com
www.linkedin.com/in/stellabridges