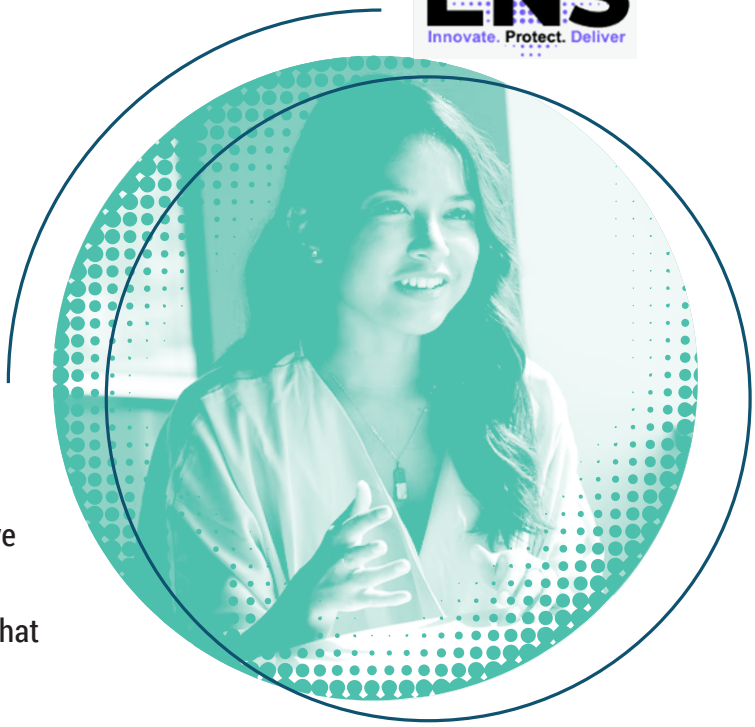
HITRUST 2023 UPDATE CHECKLIST



HITRUST

HITRUST is a leading certification in the industry.

- Founded in 2007 to help companies safeguard sensitive data and manage risk.
- Established a certifiable framework for organizations that create, access, store, or exchange covered or sensitive information.
- Originated from the belief that information security is critical to the widespread utilization of and confidence in health information systems, medical technologies, and electronic exchanges of medical data. Now, the HITRUST CSF is industry agnostic.

HITRUST CSF

- Provides organizations the ability to tailor their security control baselines when obtaining a certification to what is applicable based on their specific information security requirements.
- Incorporates both compliance and risk management principles.
- Defines a process to evaluate compliance and security risk effectively and efficiently.
- Is the framework used for HITRUST Certification.

Key Components of the CSF Assurance Program

3 high-level components associated with the HITRUST CSF:

Questionnaires

Controls applicable to your organization that are used to measure risk and compliance.

External Assessors (such as Control Case)

Uses the questionnaire to assess adherence to the HITRUST CSF.

Reports

The deliverable that can show stakeholders and customers that your organization is HITUST Certified.

2023 UPDATES TO HITRUST

HITRUST recently announced a new version of the CSF called version 11, replacing version 9.6.2.

Summary of Changes in HITRUST v11

- Added selectable compliance factors and refreshed various mappings to authoritative sources.
- Moved evaluative elements from the Policy Illustrative Procedure to the Requirement Statement.
- Updated Illustrative Procedure Content.
- Performed assorted errata updates consistent with the CSF Versioning Policy.

New Certification: e1 Assessment

- Basic cybersecurity hygiene.
- Less than 50 requirement statements.
- Annual certification.
- Quicker assurance.

HITRUST ASSESSMENT

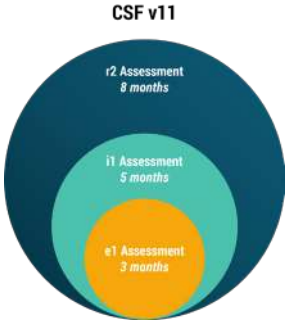
Complete portfolio of the types of HITRUST assessments and certifications:

Assessment Type	# of HITRUST Requirements	Subject Matter / Focus	Control Maturity Levels
HITRUST Essentials e1 Assessment *(valid for 1 year)*	Less than 50	**Requirements addressing:** • Basic cybersecurity hygiene • The most critical cyber threats (e.g., ransomware, phishing, password stuffing)	Implemented only But: Some requirements are P&P-focused
HITRUST Implemented i1 Assessment *(valid for 1 year)*	Approx. 180 (v11) 219 (v9.6.2)	**All requirements in the e1, PLUS:** • Leading cybersecurity practices • Requirements mapping to the even more cyber threats	Implemented only But: Some requirements are P&P-focused
HITRUST Risk-Based r2 Assessment *(valid for 2 years)*	Varied based on risk and compliance factors	**All requirements in the e1 and i1, PLUS:** • Requirements addressing inherent risk factors • Requirements addressing added compliance factors (e.g., HICP, GDPR)	Must: Policy, Procedure, Implemented Optional: Measured & Managed

Assessment Sub-type	Can Result in a Certification?	Needs an External Assessor?	QA'd by HITRUST?	Share-able via RDS?	Results in a HITRUST-issued PDF?
Readiness	No	No	No	Yes	Optional
Validated	Yes	Yes	Yes	Yes	Yes

5 maturity levels within the CSF when it comes to testing:

Policy | **Procedure** | **Implemented** | **Measured** | **Managed**



A **readiness assessment** is typically not a certification. It's a self-assessment that organizations can do to identify gaps in their environment.

A **validated assessment** allows organizations to submit the assessment for HITRUST certification.

HITRUST DOMAINS

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

CONTROLCASE METHODOLOGY

ControlCase utilizes a unique 6-phase approach that places the focus on certification from the very beginning:

ABOUT CONTROLCASE

ControlCase is a CMMC RPO and a global provider of certification, cyber security, and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost-effective, and comprehensive in both on-premise and cloud environments. ControlCase offers certifications and a broad spectrum of cyber security services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC 2 Type II, ISO 27001, PCI PIN, PCI P2PE, PCI TSP, PCI SSF, CSA STAR, HIPAA, GDPR, SWIFT, and FedRAMP.