SCHNEIDER DOWNS
Big Thinking. Personal Focus.

HITRUST Assessment Types

CHARACTERISTIC	HITRUST ESSENTIALS, 1-YEAR (e1) ASSESSMENT FOUNDATIONAL CYBERSECURITY	HITRUST IMPLEMENTED, 1-YEAR (i1) ASSESSMENT LEADING PRACTICES	HITRUST RISK-BASED, 2-YEAR (r2) ASSESSMENT EXPANDED PRACTICES
Purpose	Provides entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place	Provides a moderate level of assurance that addresses cybersecurity leading practices and a broader range of active cyber threats than the e1 assessment	A high level of assurance that focuses on a comprehensive risk-based specification of controls with an expanded approach to risk management and compliance evaluation
Number of HITRUST CSF Requirements on a 2-Year Basis	44 (Year 1), 44 (Year 2)	182 (Year 1), ~60 (Year 2 with Rapid Recertification)	~375 Average (Year 1), ~40 Average (Year 2 Interim Assessment)
Readiness assessments and validated assessments (certifications) can be performed	Yes		
Length of certification	1 year	1 year, 2 years with Rapid Recertification	2 years, with Interim Assessment
Maturity Levels Considered	Implemented	Implemented	Policy, Procedure, and Implemented
Policy and Procedure Consideration	Minimal	Minimal	Thorough
Level of Security Assurance	Low	Moderate	High
Flexibility of Control Selection (Can be tailored to optionally convey assurances over dozens of information protection regulations and standards (e.g., HIPAA, NIST CSF, PCI DSS).	No Tailoring	No Tailoring	Tailoring
Evaluation Approach	1x5: Implementation control maturity level	1x5: Implementation control maturity level	3x5 or 5x5: Control maturity assessment against either 3 or 5 maturity levels
HITRUST CSF requirements performed by the assessed entity's third party service providers (such as cloud service providers) on behalf of the organization can be carved out / excluded from consideration	Yes	Yes	No
Requires an Authorized HITRUST External Assessor Organization to inspect documented evidence to validate control implementation	Yes		
Leverages the HITRUST Control Maturity Scoring Rubric	Yes		
Final reports resulting from the assessment can be shared through the HITRUST Assessment Xchange and assessment results can be shared through the HITRUST Results Distribution System (RDS)	Yes		
Can result in a HITRUST-issued certification over the NIST Cybersecurity Framework	No	No	Yes
Can be bridged through a HITRUST bridge certificate	No	No	Yes
Threat-adaptive assessment	Yes		
Assessor's validated assessment fieldwork window (maximum)	90 days		
Alignment with Authoritative Sources	CISA Cyber Essentials, Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations, NIST 171's Basic Requirements, NIST IR 7621	NIST SP 800-171 (Basic and Derived Requirements), HIPAA Security Rule, and HICP for Medium-Sized Organizations	NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, PCI DSS, GDPR, and Dozens of Others
Must use the most current version of the CSF available at time of assessment creation.	Yes	Yes	No