



New HITRUST Implemented, 1-year (i1) Validated Assessment

Threat-adaptive Assessment Maintains Cyber Relevance Over Time as Threats Evolve and New Risks Emerge



HITRUST® is addressing the need for a continuously relevant cybersecurity assessment that aligns and incorporates best practices and leverages latest threat intelligence to stay ahead of information security risks and emerging cyber threats, such as ransomware and phishing. The unique HITRUST design, control selection, and assurance program establish the HITRUST i1 Validated Assessment in a new class of information security assessment that is threat-adaptive – designed to maintain relevance over time as threats evolve and new risks emerge.

Most existing assessment approaches are not designed to keep pace with current and emerging threats; those that do rely heavily on broad control requirements that raise questions about the suitability of controls and the consistency of review that ultimately impacts the reliability of results. In contrast, HITRUST identifies information security controls relevant to mitigating known risks and leverages cyber threat intelligence data to influence the selection – and where necessary, updating – of technically-focused HITRUST CSF® framework requirements included in the i1 Assessment. As a result, the HITRUST i1Assessment includes controls selected to address emerging cyber threats active today and will be updated regularly to address new threats in the future.

	HITRUST Implemented, 1-year (i1) Validated Assessment
Description	Validated Assessment + Certification
Purpose (Use Case)	A threat-adaptive assessment focused on best security practices with a more rigorous approach to evaluation, which is suitable for moderate assurance requirements
Targeted Coverage	NIST SP 800-171, HIPAA Security Rule, GLBA Safeguards Rule, U.S. Department of Labor EBSA Cybersecurity Program Best Practices, Health Industry Cybersecurity Practices (HICP)
Number of Control Requirement Statements	219 pre-set (static) controls that leverage security best practices and threat intelligence*
Flexibility of Control Selection	No Tailoring
Evaluation Approach	1x5: Control Implementation Only
Level of Effort / Level of Assurance Conveyed	Moderate (Relative to HITRUST Risk-based 2-year r2 Certification)
Certifiable Assessment	Yes, 1 -year
Allows for 4th Party Carve Outs (Control Requirements Performed by Subservice Providers)	Yes
Addresses Shared Responsibilities Via Internal and External Inheritance	Yes
Shares Assessment Results with Relying Parties through the HITRUST Results Distribution System™	Yes

*A HITRUST i1 Validated Assessment performed using the HITRUST CSF v9.6 framework includes 219 control requirements, however to address emerging cyber threats in the future, the number of requirements included in i1Assessments may change over time.

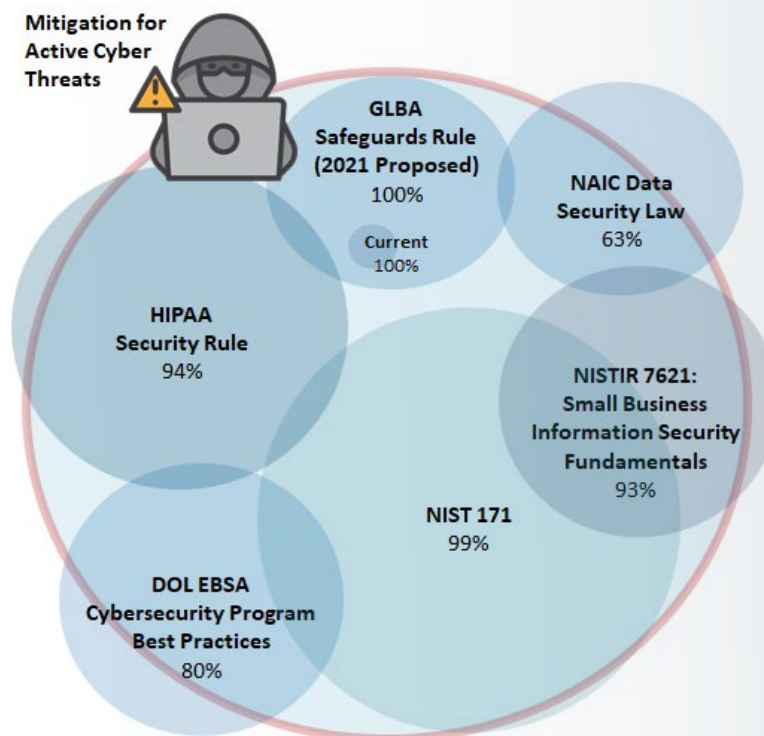
The HITRUST i1 Validated Assessment is the First Information Security Assessment of its Kind with Attributes Not Available through other Assurance Programs:

- Designed to maintain relevant control requirements to mitigate existing and emerging threats including ransomware and phishing.
- Designed to sunset controls that have lost relevance and have limited assurance value based on the effort required to comply or assess.
- Leverages the latest threat intelligence to guide future control requirements without impacting assessed entities or assessors currently working towards certification.
- Organizations with a HITRUST i1 Certification will not be impacted by future updates to the i1 Assessment control requirements until their next HITRUST Assessment cycle.
- Unique design, control selection, and rigorous HITRUST Assurance Program delivers higher reliability than comparable assurance options.
- Uses HITRUST patent pending Assurance Intelligence Engine™ to identify errors, omissions, and potential fraud.
- Shares results with relying parties through the HITRUST Results Distribution System (RDS).
- Provides stronger assurances than comparable assessments with a similar level of time and effort.
- Offers a forward-looking, 1-year certification.

i1 Assessment is Based on Proven HITRUST CSF Requirements

Since the HITRUST i1 Assessment is designed around relevant information security risks and emerging cyber threats, it includes a combination of *good security hygiene controls* and *best-practice controls* from the HITRUST CSF framework. This control selection predictably maps and provides a high degree of coverage to other standards or authoritative sources generally viewed as security best practices, such as NIST SP 800-171, HIPAA Security Rule, GLBA Safeguards Rule, U.S. Department of Labor EBSA Cybersecurity Program Best Practices, Health Industry Cybersecurity Practices (HICP); as well as the HITRUST CSF framework requirements included in the HITRUST Basic, Current-state (bC) Assessment.

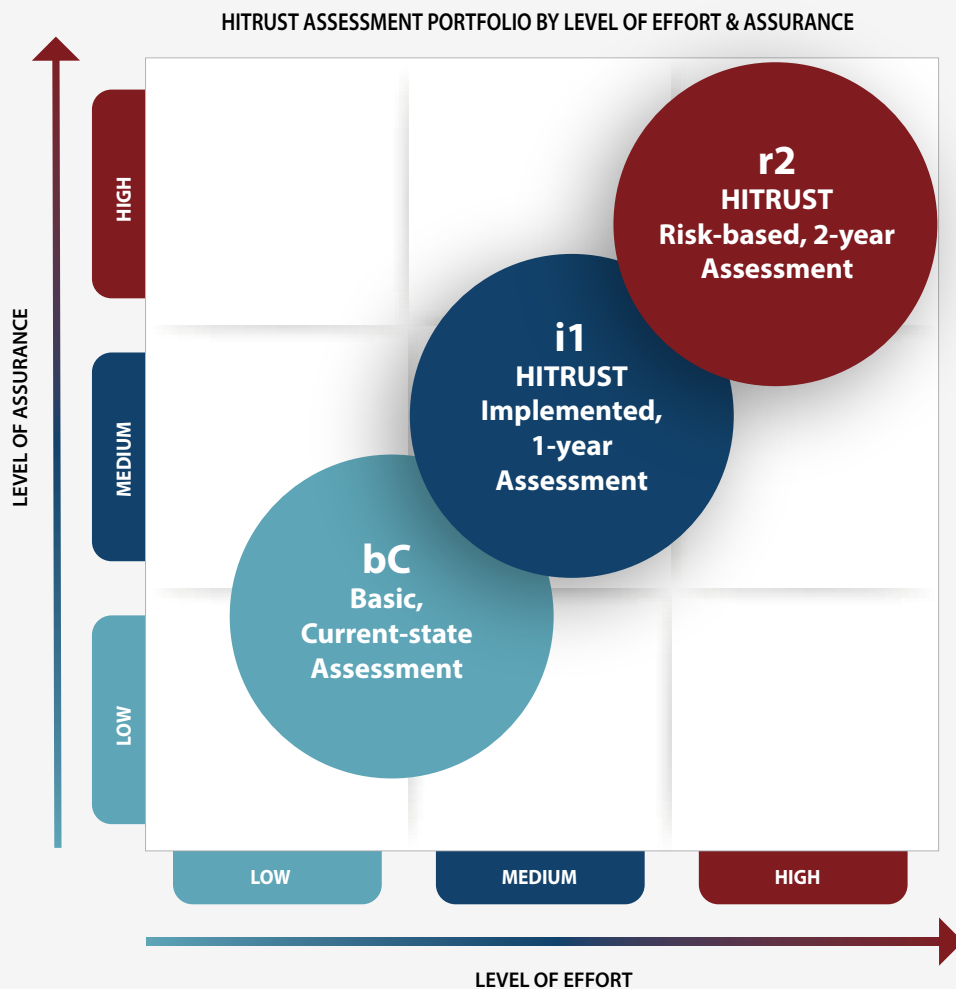
The diagram below shows the coverage provided by the controls included in the i1 Assessment performed against v9.6 of the HITRUST CSF. (Note: The graphic focuses on the coverage amounts provided by the i1 Assessment and is not meant to represent the overlap between the Authoritative Sources.)



To ensure the control selection for the i1 Assessment remains relevant over time, HITRUST will evaluate security controls and review threat intelligence data no less than quarterly and for each subsequent major and minor release of the HITRUST CSF framework. Guidance documents will also drive enhancements to the HITRUST CSF and HITRUST i1 Assessment control sets as needed. While the HITRUST i1 Assessment is intended to adapt and evolve to maintain relevance, it's important to note that organizations with a HITRUST i1 Certification will not be impacted by changes to the HITRUST i1 Assessment control requirements until their next HITRUST assessment cycle.

How the i1 Fits into the Full HITRUST Assessment Portfolio

All HITRUST assessments leverage a single assurance methodology, framework, assessment platform, and the HITRUST Results Distribution System. This approach ensures consistency and efficiency across the assessment portfolio. In addition, it simplifies supporting varying levels of assurance and allows for assessed entities to more easily transition to higher levels of assurance as their programs mature.



All HITRUST assessments aid in understanding the effectiveness of an organization's cyber preparedness and resilience. Compared to other HITRUST assessments, the Implemented 1-year i1 Assessment delivers a relatively moderate level of assurance and falls between the HITRUST bC Self-assessment and the HITRUST Risk-based 2-year r2 Assessment.

HITRUST bC Assessment. Focuses on *good security cyber hygiene* controls that are right for any sized organization with a simple approach to evaluation, which is suitable for scenarios requiring rapid and/or lower levels of assurance. The bC is a verified self-assessment that leverages the patent pending HITRUST Assurance Intelligence Engine to identify errors and omissions to pinpoint problems so they can be fixed before completion.

HITRUST r2 Validated Assessment. Formerly named the HITRUST CSF Validated Assessment, this assessment focuses on a comprehensive risk-based, tailorable set of controls suitable for scenarios requiring a highly rigorous approach requiring strong assurances. r2 Certifications are valid for 2 years.

Due to the transparency and consistency of how the controls are selected, scored, and validated by qualified third-party external assessors and the HITRUST Assurance and Quality teams, the HITRUST i1 and r2 Assessments provide higher levels of assurance than the bC Self-assessment. However, the level of effort required for an i1 Certification is significantly less than an r2 Certification due to fewer control requirement statements and fewer maturity levels in the i1 (Implementation only).

Similarities and Differences Between the i1 and r2 Certifications

The HITRUST Implemented, 1-year i1 Certification shares several characteristics with the HITRUST Risk-based, 2-year r2 Certification.

Similarities

- Both i1 and r2 Assessments provide an effective way to convey information assurances over the assessed entity's scoped control environment through shareable, final results with certification issued by HITRUST
- Readiness Assessments and Validated Assessments can be performed for both.
- Both require an Authorized HITRUST External Assessor Organization to inspect documented evidence to validate control implementation.
- Both undergo full Quality Assurance (QA) by HITRUST.
- Both use requirements included in the HITRUST CSF and both use the HITRUST MyCSF® SaaS best in class information risk management platform.
- The HITRUST i1 and r2 Validated Assessment Reports can be shared with assessed entities and relying parties by the HITRUST Results Distribution System via a PDF, web browser, and/or API.
- Both can be shared through the HITRUST Assessment XChange™.

Differences

- Relative to an r2 Assessment, an i1 Assessment requires less effort and time to complete.
- When scoring HITRUST CSF requirements included in r2 Assessments, control maturity levels are considered for Policy, Process, Implemented, and optionally Measured and Managed; while the scoring of HITRUST CSF requirements included in i1 Assessments consider only control Implementation.
- r2 certifications are valid for 2 years, while i1 certifications are valid for 1 year. Consequently, no interim or bridge assessment is necessary for the i1.
- While the HITRUST CSF requirements considered in r2 Assessments are tailored based on the assessed entity's inherent risk factors (examples: whether in-scope systems are accessible from the Internet, whether wireless networks are used in the scoped environment, etc.), the HITRUST CSF requirements in an i1 Assessment are carefully curated by HITRUST and may vary only when performed against different versions of the HITRUST CSF.
- r2 Assessments can be tailored to optionally convey assurances over dozens of information protection regulations and standards (including HIPAA, NIST CSF, PCI DSS, and more), while i1 Assessment controls are pre-set.
- While r2 Assessments can be tailored to include all security control references present in the HITRUST CSF through use of the "comprehensive assessment" option, i1 Assessments cannot.
- HITRUST CSF requirements performed by the assessed entity's service providers (such as cloud service providers) on behalf of the organization can be carved out / excluded from consideration in i1 Validated Assessments, but such carve-outs are not permitted in r2 Assessments.

- A NIST Scorecard is included in the r2 Validated Assessment Report detailing the organization's compliance with NIST Cybersecurity Framework-related controls included in the HITRUST CSF framework, but is not included in an i1.
- The MyCSF Compliance and Reporting Pack for HIPAA is available to use during an r2 Assessment, but not during an i1 Assessment.

Benefits of a HITRUST i1 Certification

- **The most trusted results available** for moderate assurance levels due to suitability of controls, the rigor of assurance program, and centralized oversight because HITRUST QAs 100% of i1 and r2 Validated Assessments and is the sole issuing body of all HITRUST certifications.
- The i1 **will satisfy assurance needs** of internal and external stakeholders—**Assess Once, Report Many™**.
- HITRUST performs **full QA on 100%** of r2 and i1 Validated Assessments and is the sole issuing body of all HITRUST certifications.
- The i1 **provides a competitive advantage** for strengthening existing business relationships and earning new business partnerships.
- The **threat-adaptive and continuously relevant** nature of the i1 Validated Assessment can help justify a **reduction in cyber insurance premiums**.
- **Will use the HITRUST Results Distribution System** to share results more efficiently with assessed entities and relying parties.
- **Adds peace-of-mind** that your organization's data networks and IT assets are protected from intrusion and breaches.
- Since some organizations choose an i1 Assessment based on speed-to-completion considerations, HITRUST has established a **45 business days** (or less) post-submission Service Level Agreement **to complete QA on Validated i1 Assessments**—or the customer's next i1 Validated Assessment report credit is free. (Note: Validated assessment submissions that enter escalated QA due to quality concerns are exempted from this SLA.)



**For More Information about the i1 Validated Assessment:
Contact your HITRUST Product Specialist**

Call: 855-448-7878 or Email: sales@hitrustalliance.net

