## i1 Leading Security Practices Assessment Delivers Broad and Reliable Assurances Against Current and Emerging Cyber Threats

The HITRUST Implemented, 1-Year (i1) Validated Assessment leverages a proven set of HITRUST-curated controls designed to ensure that an organization is exercising *Leading Security Practices*. The i1 Assessment provides reliable assurances against current and emerging cyber threats to help implement a strong and broad cybersecurity program.

Cyber Threat-Adaptive Approach for Added Protection

The HITRUST CSF® framework enables the entire HITRUST assessment portfolio to leverage cyber threat-adaptive controls that are appropriate for each level of assurance – including the i1. HITRUST analyzes trending cyber threat intelligence data to maintain relevant control requirements that are designed to mitigate new and emerging risks, including phishing, brute force, and ransomware.
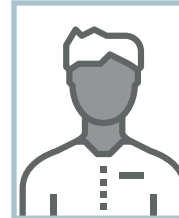
Assures Broader Protection
" The i1 gives our stakeholders confidence we're meeting leading security practices now and in the future."

Operational Focus and Inheritance Reduce Effort and Accelerate Certification

The i1 includes pre-set control requirements that enable organizations to demonstrate the operational maturity of their cybersecurity program. The i1 focuses on implementation and allows for control carve-outs or inclusion of controls performed by third-party service providers. Organizations that choose to include third-party controls can use inheritance to significantly reduce the level of effort associated with testing controls. These capabilities focus on operational security system performance to reduce the complexity and time needed to measure program maturity.

Unique Attributes of the HITRUST i1 Assessment
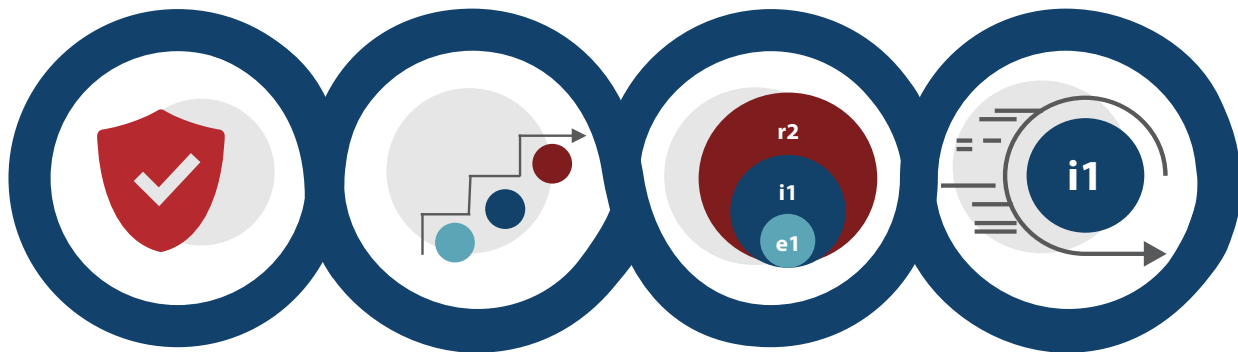
LEADING SECURITY PRACTICES
Supports a complete cybersecurity program that evolves based on regular analysis of threat intelligence data.

HIGHER RELIABILITY
Provides stronger assurances than comparable assessments with a similar level of time and effort.

STREAMLINES ASSESSMENT PROCESS
Focuses on implementation to practically assess information security operational maturity with greater efficiency.

RAPID RECERTIFICATION
Dramatically simplifies the i1 recertification process.

USE CASES: The i1 Offers the Right Level of Assurance for Many Organizational Needs

i1 as the Final Destination
- For reliable measurement and assurance against robust cybersecurity controls.
- To demonstrate broad protection against current and emerging threats, which can help meet contractual and compliance obligation
- To show justification for more favorable cyber insurance premiums.

i1 as a Stepping-Stone
- When organizations need a certification step while on the path to a HITRUST r2.

i1 for Third-Party Risk Management
- To ensure that business partners are using leading security practices for reliable information protection.
- To establish a meaningful benchmark for third-party service providers progressing their cybersecurity programs.

Key i1 Highlights

- Leverages current threat intelligence trend data to update control requirements and proactively defend against emerging threats.
- Adds efficiency with *nested* controls in the traversable HITRUST CSF framework, which allows the i1 to inherit control scoring from the e1 and provide inheritable (implemented) control scoring for the r2.
- Focuses on the control implementation maturity level.
- Provides a 1-year Certification.
- Includes an i1 Readiness Assessment option to prepare for an i1 Validated Assessment + Certification
- Rapid Recertification reduces effort and accelerates obtaining the next i1 1-year Certification by sampling and evaluating ~60 requirement statements scored in previous full i1 Assessment.

How the i1 Fits into the HITRUST Assessment Portfolio

r2 *Expanded Practices*

i1 *Leading Practices*

e1 *Essentials*

The Implemented, 1-Year i1 Assessment falls between the HITRUST e1 Essentials 1-Year Assessment and the HITRUST Risk-based 2-year r2 Assessment. With an extensive set of additional requirement statements, the i1 addresses a broader range of active cyber threats than the e1 Essentials Assessment. HITRUST considers the i1 to be a moderate level of assurance relative to the HITRUST r2 Certification, and the r2 continues to provide the highest level of security assurance.

i1 IMPLEMENTED 1-YEAR
HITRUST® CERTIFIED

HITRUST i1 Readiness and Validated Assessments Offer Multiple Paths to Reach a Leading Security Practices Level of Information Protection Assurance

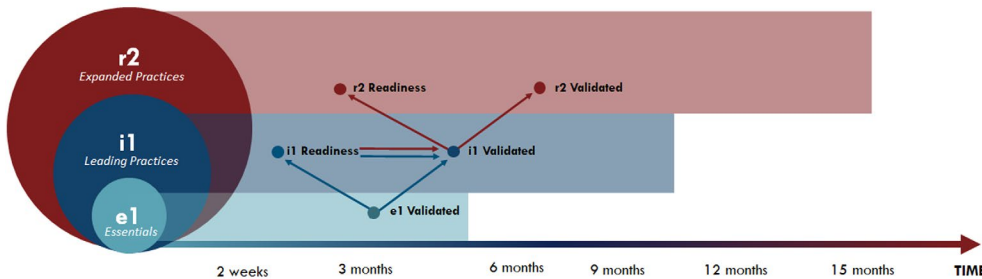**i1 PATH 1:** The i1 is the final assurance destination

    Option 1: Start with an e1 ➤ progress to an i1

    Option 2: Start with an i1 Readiness Assessment ➤ progress to the i1 Validated Assessment

i1 PATH 2: Use the i1 as a stepping-stone to the r2 as the final assurance destination

    Option 1: Start with an i1 Readiness Assessment ➤ progress to the i1 Validated Assessment ➤ progress to the r2

    Option 2: Start with an i1 Validated Assessment ➤ progress to the r2

r2 *Expanded Practices*

i1 *Leading Practices*

e1 *Essentials*

r2 Readiness — r2 Validated

i1 Readiness — i1 Validated

e1 Validated

2 weeks   3 months   6 months   9 months   12 months   15 months   **TIME**

Enables Continuous Improvement

"We use the i1 as part of a progressive plan to achieve HITRUST r2 Certification."

i1 At-A-Glance Overview

Description	HITRUST Implemented, 1-year (i1) Assessment *Leading Practices*
	Validated Assessment + Certification
Purpose (Use Case)	Provides a moderate level of assurance that **addresses cybersecurity leading practices** and a broader range of active cyber threats than the e1 assessment
Number of HITRUST CSF Requirements on a 2-Year Basis and Maturity Levels Considered	182 (Year 1), ~60 (Year 2 with Rapid Recertification), Implemented
Policy and Procedure Consideration	Minimal
Flexibility of Control Selection	No Tailoring
Evaluation Approach	1x5: Implementation control maturity level
Level of Assurance Conveyed	Moderate, (relative to r2 Certification)
Control Requirements Performed by Service Providers	Allows Carve-Outs or Inclusion
Certifiable Assessment	Yes, 1 Year + Rapid Recertification in Year 2
Supporting Assessments	Readiness, Rapid Recertification
Aligned Authoritative Sources	NIST SP 800-171 (Basic and Derived Requirements), HIPAA Security Rule, and HICP for Medium-Sized Organizations
Provides Targeted Coverage for One or More Authoritative Sources	No
Uses the HITRUST Results Distribution System™ to Share Results	Yes
Leverages HITRUST Assurance Intelligence Engine™ (AIE) to Prevent Omissions and Errors	Yes

Types of i1 Assessments

Readiness Assessment. Organizations may use a Readiness Assessment to prepare for a future i1 Validated Assessment + Certification. This can be a self-assessment or can be facilitated by an External Assessor. HITRUST generates a standard report and compliance scorecard for the Readiness Assessment, however i1 Readiness Assessment results are not validated and therefore provide a limited level of security assurance. If needed, Corrective Action Plans (CAPs) can be identified during a Readiness Assessment.

Validated Assessment + Certification. The i1 provides reliable leading practices assurances for information risk management due to its strong assessment approach, which meets the demands of multiple internal and external stakeholders.

Validated Assessment. An i1 Validated Assessment Report is issued from HITRUST if an i1 Assessment does not meet the certification scoring threshold criteria in one (or more) domains. A Validated Assessment can be a stepping-stone to earn full certification.

Rapid Recertification. Requires sampling only a fraction of control requirement statements, which reduces the effort and cost to earn a second 1-year Certification.

THIRD-PARTY RISK MANAGEMENT (TPRM)
The i1 – along with HITRUST e1 and r2 Assessments – Provide Excellent Assurance Options to Reduce Vendor Information Security Risk

Multiple industry studies report that 50% or more of data breaches are caused by third- and even fourth-party vendors. That's why it is critical to protect your organization by obtaining information security assurances from business partners with whom you share online networks or sensitive data.

The HITRUST i1 Assessment allows relying parties to request a reliable information protection assurance from their business partners against a broad set of controls that demonstrate leading security practices. It also provides an excellent way for vendors to get started on the path to an r2.
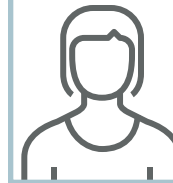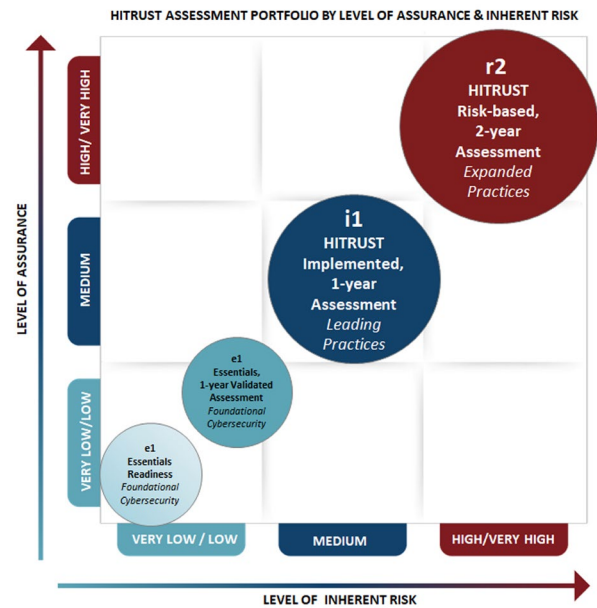
Reduces Vendor Risk

"*Requesting an i1 from key vendors helps us identify and manage data security risk more effectively.*"

Choosing the Right HITRUST Assessment to Request from Vendors Based on Their Level of Inherent Risk

Inherent Risk Score*	Required Level of Assurance	Assessment Needed
5	Very High	**r2 Validated**
4	High	**r2 Validated** (CAPS Allowed)
3	Moderate	**i1 Validated** (CAPS Allowed)
2	Low	**e1 Validated** (No CAPS)
1	Very Low	**e1 Readiness**
0	Negligible	N/A

*Based on inherent risk scoring, the i1 Validated Assessment is designed for third parties that require a **moderate level of assurance**.

The HITRUST Risk Triage Methodology quantifies, scores, and qualifies the level of risk inherent in sharing information with a third party, which then translates into determining the appropriate assessment needed.
For more information, refer to the HITRUST TPRM Implementation Handbook.

HITRUST ASSESSMENT PORTFOLIO BY LEVEL OF ASSURANCE & INHERENT RISK

LEVEL OF ASSURANCE

HIGH/ VERY HIGH

MEDIUM

VERY LOW/LOW

r2 HITRUST Risk-based, 2-year Assessment *Expanded Practices*

i1 HITRUST Implemented, 1-year Assessment *Leading Practices*

e1 Essentials, 1-year Validated Assessment *Foundational Cybersecurity*

e1 Essentials Readiness *Foundational Cybersecurity*

VERY LOW / LOW   MEDIUM   HIGH/VERY HIGH

LEVEL OF INHERENT RISK

Vendor assurance reporting and progress can be monitored through the HITRUST Results Distribution System.

The Innovative HITRUST Approach Improves Efficiency and Consistency Across the HITRUST Assessment Portfolio

- **HITRUST CSF® framework** enables a traversable assessment journey to progressively achieve higher assurance levels by sharing common control requirements.
- **Control Inheritance** in the HITRUST MyCSF® platform saves time, effort, and money by allowing the reuse of scoring work and comments from prior HITRUST e1, i1, or r2 Assessments.
- **HITRUST Assessments** offer *Assess Once, Report Many*™ benefits by meeting multiple requirements and minimizing the need for additional reports.
- **HITRUST Assurance Program™** ensures an unparalleled level of accuracy and trust with a consistent, centralized, and comprehensive assessment methodology.
- **HITRUST Assessment XChange™** provides Third-Party Risk Management (TPRM) services to assist Participating Organizations in assessing and evaluating their vendors' information security programs.

To Discuss How the HITRUST Leading Practices, 1-year i1 Validated Assessment + Certification Can Help Improve Your Information Security Program and Assist with Third-Party Information Risk Management
Call: 855-448-7878 or Email: sales@hitrustalliance.net