HITRUST®

Essentials, 1-year (e1) Validated Assessment
Foundational Cybersecurity

e1 Essentials Assessment Adds Efficiency and Flexibility to the HITRUST Portfolio

Adding the HITRUST Essentials, 1-Year (e1) Validated Assessment + Certification to the i1 and r2 assessment options broaden the HITRUST portfolio coverage across a wide range of assurance needs. The e1 targets lower-risk organizations or can be a starting point for enterprises that are in the early stages of implementing their information security controls.

Faster, More Streamlined Assurances

To ensure *Foundational Cybersecurity* is in place, the e1 focuses only on essential information security controls. The selection of controls curated by HITRUST is intended to address fundamental cybersecurity practices, and was influenced by authoritative sources sharing similar goals, such as CISA Cyber Essentials, Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations, NIST 171's Basic Requirements, and NIST IR 7621.
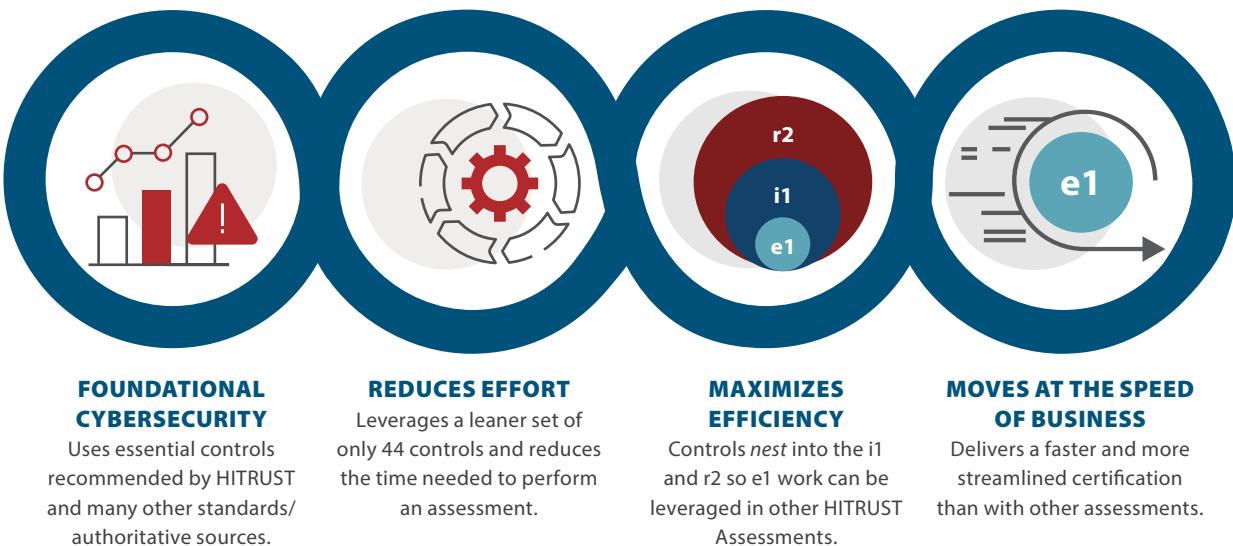
Focusing on the Basics
"The e1 is an efficient way to show that our core cybersecurity controls are operating effectively to protect the organization."

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 e1. HITRUST analyzes trending cyber threat intelligence to maintain relevant control requirements that are designed to mitigate new and emerging risks including phishing, brute force, and ransomware.

Unique Attributes of the HITRUST e1 Assessment

FOUNDATIONAL CYBERSECURITY
Uses essential controls recommended by HITRUST and many other standards/ authoritative sources.

REDUCES EFFORT
Leverages a leaner set of only 44 controls and reduces the time needed to perform an assessment.

MAXIMIZES EFFICIENCY
Controls *nest* into the i1 and r2 so e1 work can be leveraged in other HITRUST Assessments.

MOVES AT THE SPEED OF BUSINESS
Delivers a faster and more streamlined certification than with other assessments.

USE CASES: The e1 Offers the Right Level of Assurance for Many Organizational Needs

e1 as the Final Destination

- As a reliable information security assurance to demonstrate that low-risk enterprises have foundational cybersecurity in place.
- As a faster assessment option to obtain assurances, establish benchmarks, and identify coverage gaps.
- For small organizations or start-ups to differentiate themselves in the marketplace.
- To get meaningful assurance reports for Merger/Acquisition partners, new business units, or recently deployed technology platforms.
- To show justification for more favorable cyber insurance premiums.

e1 as a Stepping-Stone

- For organizations that need additional time to implement the more robust control environment needed for HITRUST i1 or r2 Assessments.
- As a milestone to demonstrate progress towards an i1 or r2.
- For enterprises that are new to HITRUST to get started.

e1 for Third-Party Risk Management

- To evaluate or onboard third-party business partners.
- To request assurances from service providers who handle limited-PII business processes, such as: Sales/Marketing Agencies, Call Centers, Facility Managers, Research Partners, Insurance Brokers, Financial Brokers, Advisors, Auditors, and Others.

Key e1 Highlights

- Leverages current threat intelligence trend data to update control requirements and proactively defend against emerging threats.
- Accelerates and simplifies the journey to stronger assurances by allowing reuse of e1 work in other HITRUST assessments.
- Unlike typical questionnaires, provides a scored and validated assessment over key controls curated by HITRUST, which offers more in-depth and *Rely-Able™* assurances to stakeholders.
- Uses a consistent methodology and framework to enhance expertise of operational teams and stakeholders.
- Focuses on the control implementation maturity level.
- Provides a 1-year Certification.
- Includes an e1 Readiness Assessment option to prepare for an e1 Validated Assessment + Certification.

How the e1 Fits into the HITRUST Assessment Portfolio

r2 *Expanded Practices*

i1 *Leading Practices*

e1 *Essentials*
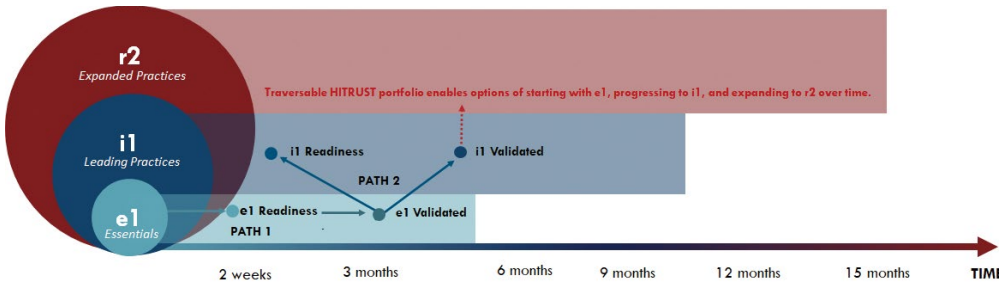
The e1 Essentials Assessment requires less effort to complete and falls below the level of assurance conveyed by the more rigorous HITRUST i1 and r2 Assessments. The e1 provides the right level of assurance for organizations that pose low levels of risk. The e1 also provides an excellent starting point for progressing to a higher assurance level. The e1 Readiness Assessment can be used to prepare for a future e1 Validated Assessment + Certification.

e1 ESSENTIALS 1-YEAR HITRUST® CERTIFIED

HITRUST e1 Essentials Readiness and Validated Assessments Provide Multiple Paths to Success

e1 PATH 1: Final assurance destination for organizations posing low levels of risk
e1 PATH 2: Starting point to higher levels of HITRUST assurance

r2 *Expanded Practices*

i1 *Leading Practices*

e1 *Essentials*

Traversable HITRUST portfolio enables options of starting with e1, progressing to i1, and expanding to r2 over time.

i1 Readiness → i1 Validated
PATH 2

e1 Readiness → e1 Validated
PATH 1

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

A Great Starting Point
"As we continue to mature our cybersecurity program, the e1 is an excellent building block to the next assurance level."

e1 At-A-Glance Overview

Description	HITRUST Essentials 1-year (e1) Assessment *Foundational Cybersecurity* Validated Assessment + Certification
Purpose (Use Case)	Provides entry-level assurance focused on the most critical cybersecurity controls to demonstrate that **essential security hygiene** is in place
Number of HITRUST CSF Requirements on a 2-Year Basis and Maturity Levels Considered	44 (Year 1), 44 (Year 2), Implemented
Policy and Procedure Consideration	Minimal
Flexibility of Control Selection	No Tailoring
Evaluation Approach	1x5: Implementation control maturity level
Level of Assurance Conveyed	Low (for organizations that present a low level of information security risk)
Control Requirements Performed by Service Providers	Allows Carve-Outs or Inclusion
Certifiable Assessment	Yes, 1-year
Supporting Assessments	Readiness
Alignment with Authoritative Sources	CISA Cyber Essentials, Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations, NIST 171's Basic Requirements, NIST IR 7621
Provides Targeted Coverage for One or More Authoritative Sources	No
Uses Results Distribution System™ to Share Results	Yes
Leverages HITRUST Assurance Intelligence Engine™ (AIE) to Prevent Omissions and Errors	Yes

THIRD-PARTY RISK MANAGEMENT (TPRM)
The e1 Essentials – along with HITRUST i1 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 e1 Assessment allows relying parties to request a less demanding assessment from business partners who pose a lower level of inherent risk. It also provides an excellent way for vendors to get started towards a higher level of assurance over time.

Mitigate Third-Party Risk
"Requesting an e1 is ideal to help onboard lower risk vendors and evaluate business partners with greater confidence."
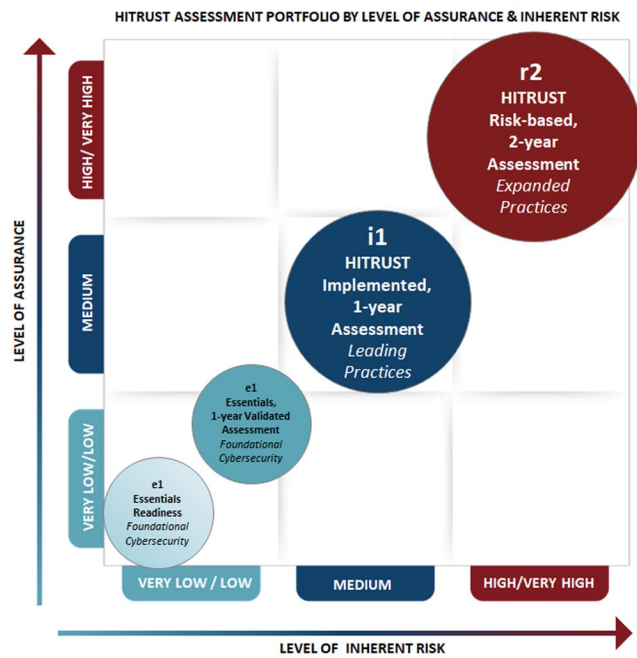
Choosing the Right HITRUST Assessment to Request from Vendors Based on Their Level of Inherent Risk

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 e1 Validated Assessment is designed for third parties that require a *low level of assurance* and an e1 Readiness Assessment is designed for third parties that require a *very low 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 Essentials, 1-year e1 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