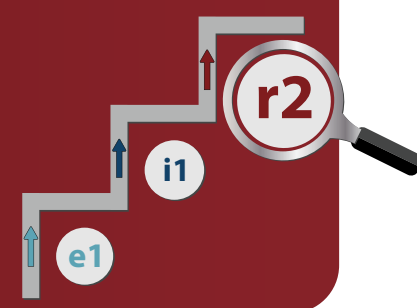


Risk-based, 2-year (r2) Validated Assessment

Expanded Practices

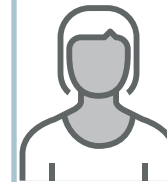


r2 Expanded Practices Assessment is the Industry-Recognized Gold Standard for Providing the Highest Level of Information Protection and Compliance Assurance

The HITRUST Risk-based, 2-year (r2) Validated Assessment demonstrates that an organization is taking the most proactive *Expanded Practices* approach to data protection and information risk mitigation. The r2 is globally recognized as a high-level validation showing that an enterprise successfully manages risk by meeting and exceeding industry-defined standards for cybersecurity.

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 r2. 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.

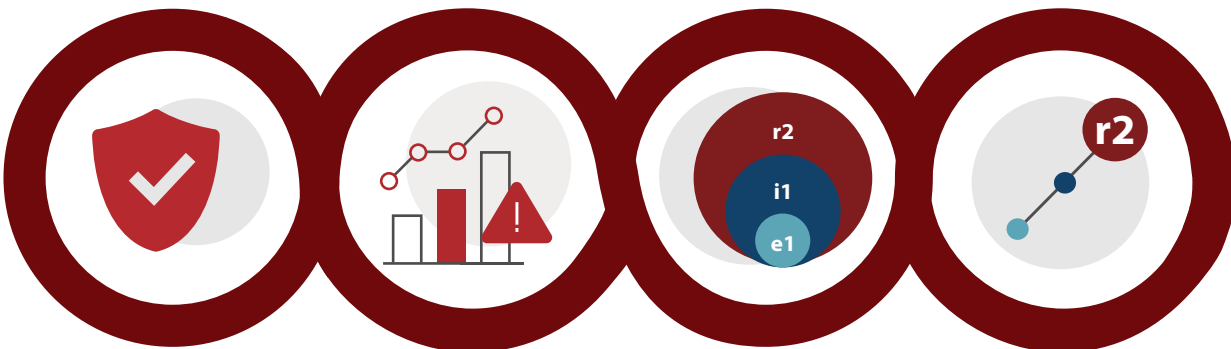


Assures Broader Protection
“We need the flexibility to tailor our assessments in different ways, so the r2 is the right choice for us.”

The Gold Standard

The HITRUST r2 Validated Assessment + Certification is considered the gold standard for information protection assurances because of the comprehensiveness of control requirements, depth of review, and consistency of oversight. The r2 offers flexible, tailorable, risk-based control selection to meet the most stringent risk and compliance factors. For organizations sharing sensitive information, handling high volumes of data, or facing challenging regulatory requirements, a properly scoped and tailored r2 Assessment ensures that control requirements are effective and compliant.

Unique Attributes of the HITRUST r2 Assessment



EXPANDED PRACTICES RELIABILITY

The HITRUST CSF® control library harmonizes with mappings to each authoritative source so the r2 delivers more precise and comprehensive cybersecurity.

RISK-BASED APPROACH

Provides tailoring to precisely select the prescriptive controls that cover whichever risk and compliance factors an organization needs.

ADDS EFFICIENCY

Requirements across the portfolio nest into each other to save time and effort by leveraging work from other HITRUST Assessments.

HIGHEST LEVEL OF ASSURANCE

r2 Certification puts organizations into an elite group by showing they meet the most demanding information risk requirements.

USE CASES: The r2 Offers the Highest Level of Assurance for the Most Demanding Organizational Needs

r2 as the Final Destination

- When assurances are needed over specific authoritative sources or international requirements.
- For organizations processing large amounts of sensitive data and personal information, including PHI.
- To *Assess Once, Report Many™* for enterprises working in multiple industries with complex regulations such as NIST, PCI DSS, HIPAA, and more.
- During an r2, the MyCSF® Compliance and Reporting Pack for HIPAA automatically compiles HIPAA compliance evidence.
- When a NIST Scorecard Report is needed to demonstrate compliance with NIST Cybersecurity Framework controls.
- When an organization's customer has adopted HITRUST as the required assurance mechanism for doing business.
- To gain a competitive advantage by strengthening business relationships.
- To show justification for more favorable cyber insurance premiums.

r2 for Third-Party Risk Management

- To request from service providers that handle PII, ePHI, and other sensitive data that requires the highest levels of assurance.
- For third-party vendors that present high levels of risk due to data volumes, regulatory compliance, or other risk factors.
- When your organization needs added confidence that a business partner provides rigorous cybersecurity protection and compliance.

Key r2 Highlights

- Leverages current threat intelligence trend data to update control requirements and proactively defend against emerging threats.
- Flexible and tailorable controls cover a wide range of industries and can be targeted for specific authoritative sources or risk factors.
- Offers the most *Rely-Able™* and highest level of information protection assurances to satisfy internal and external stakeholders.
- Delivers thorough and rigorous evaluation to accurately pinpoint control gaps and deficiencies so organizations can implement effective plans for improvement.
- Provides a 2-year Certification.
- Includes r2 Readiness, Interim, and Bridge Assessment options.

How the r2 Fits into the HITRUST Assessment Portfolio



The r2 is the only HITRUST assessment that allows fully targeted tailoring capabilities to select whichever risk factors, authoritative sources, and compliance standards are needed. Due to a comprehensive scoring approach against 3 or 5 PRISMA maturity levels, a very rigorous approach to evaluation, and more requirement statements in an r2 than an e1 or i1, the r2 Assessment consistently provides the highest level of assurance for organizations with the greatest risk exposure. Commensurate

with added assurance, the level of effort required for an r2 Certification is significantly greater than for an e1 or i1. The r2 Readiness Assessment can be used to prepare for a future r2 Validated Assessment + Certification.



HITRUST r2 Readiness and Validated Assessments Offer Multiple Paths to Reach the Highest Level of Information Protection Assurance

r2 PATH 1: Begin with a lower level HITRUST Assessment and move up to the r2

Option 1: Start with an e1 → progress to an i1 → move up to the r2

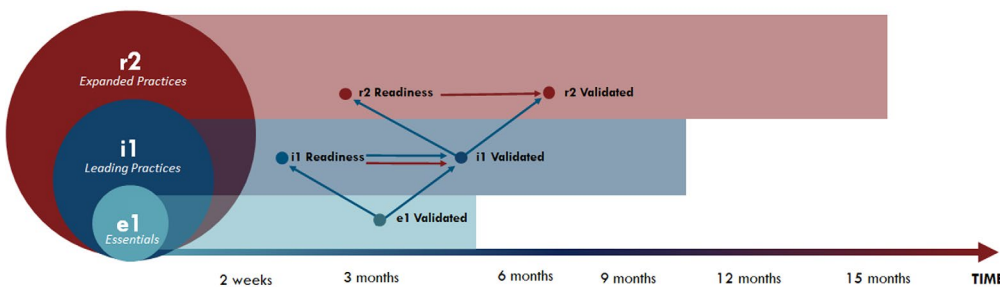
Option 2: Start with an i1 → move up to the r2

r2 PATH 2: Begin with the r2 as the final destination

Option 1: Start with an r2 Readiness Assessment → progress to the r2 Validated Assessment as the final assurance destination

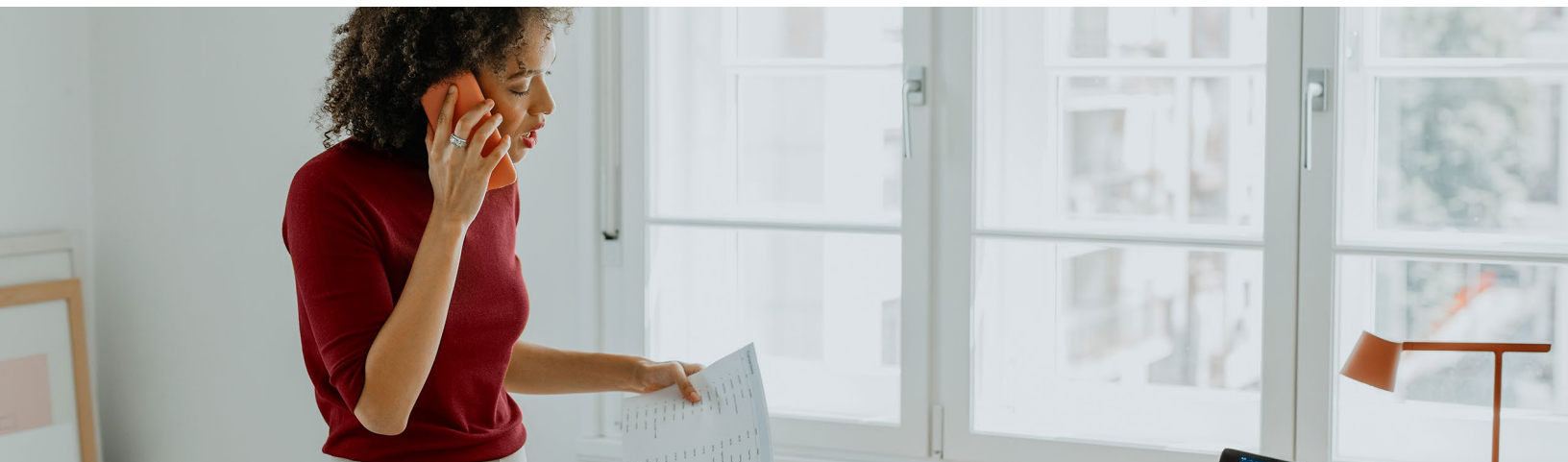
Option 2: Proceed directly to the r2 Validated Assessment as the final assurance destination

(enterprises with a mature cybersecurity program or past r2 Assessment may be able to use Option 2)





Enables Continuous Improvement
"The r2 helps ensure we fully comply with the strict cybersecurity requirements that govern our sector."





r2 At-A-Glance Overview

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

Description	Validated Assessment + Certification
Purpose (Use Case)	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 Requirement Statements on a 2-year Basis and Maturity Levels Considered	~375 Avg. (Year 1), ~40 (Year 2 Interim Assessment), Policy, Procedure, and Implemented
Policy and Procedure Consideration	Thorough
Flexibility of Control Selection	Tailoring
Evaluation Approach Level of Assurance Conveyed	3x5 or 5x5: Control Maturity assessment against either 3 or 5 maturity levels
Control Requirements Performed by Service Providers	Included
Certifiable Assessment	Yes, 2-year
Supporting Assessments	Readiness, Interim, Bridge
Aligned Authoritative Sources	NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, PCI DSS, GDPR, and dozens of others
Provides Targeted Coverage for One or More Authoritative Sources	Yes
Uses HITRUST Results Distribution System™ to Share Results	Yes
Leverages HITRUST Assurance Intelligence Engine™ (AIE) to Prevent Omissions and Errors	Yes


Types of r2 Assessments

 **Readiness Assessment.** Organizations may use a Readiness Assessment to prepare for a future r2 Validated Assessment + Certification. This can be a self-assessment or can be facilitated by an External Assessor. Although HITRUST generates a standard report and compliance scorecard, r2 Readiness Assessment results are not validated, so provide a limited level of assurance. If needed, Corrective Action Plans (CAPs) can be identified during a Readiness Assessment.


 **Validated Assessment + Certification.** The r2 is considered the gold standard in providing responsible and reliable assurances for risk management and compliance due to its rigorous, comprehensive, and effective approach, which meets the most demanding needs of multiple internal and external stakeholders.

Options for the r2 Validated Assessment + Certification:

Security Assessment	Control requirements are identified and selected based on mitigating threats and exposures that are most likely to result in a breach.
Security & Privacy Assessment	Control requirements are identified and selected based primarily upon breach risks, plus include all privacy controls.
Comprehensive Security Assessment	Includes all 135 controls in the CSF to further reduce organizational risk and demonstrate compliance.
Comprehensive Security & Privacy Assessment	Includes all 135 controls in the CSF, plus all privacy controls.

 **Validated Assessment.** An r2 Validated Assessment Report is issued from HITRUST if an r2 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.

Interim Assessment. Organizations with a HITRUST Risk-based, 2-year (r2) Validated Certification Report are required to perform an r2 Interim Assessment at the one-year mark to keep their certification valid. With a MyCSF subscription, the interim assessment is included at no additional charge.

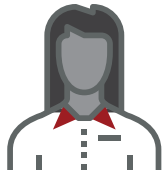
 **Bridge Assessment.** Allows organizations to earn a bridge certificate to maintain their HITRUST Risk-based, 2-year (r2) Certification Report for an additional 90 days, even if the assessment submission due date is missed.

THIRD-PARTY RISK MANAGEMENT (TPRM)

The r2 – along with HITRUST e1 and i1 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 r2 Assessment** serves as the gold standard assurance to request from vendors and service providers handling significant volumes of PII, ePHI, and other sensitive data so your organization can be fully confident that shared information stays protected.



Reduces Vendor Risk
"Our service providers process sensitive PII for us, so we require them to use the r2."

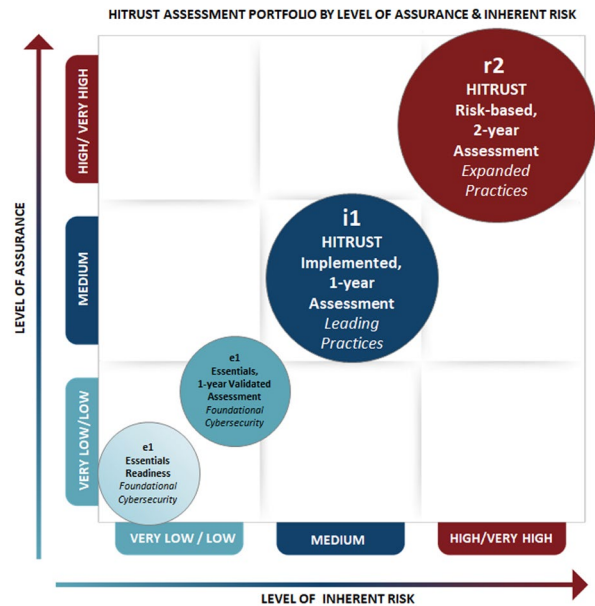
Choosing the Right HITRUST Assessment to Request from Vendors Based on Their Level of Inherent Risk

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 r2 Validated Assessment is designed for third parties that require a **high level of assurance** or a **very high 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](#).



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 Expanded Practices, 2-year r2 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