HITRUST

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

The Industry-Recognized Gold Standard for Providing the Highest Level of Information Protection and Compliance Assurance

With ever-evolving cyberthreats, organizations need to confirm they use effective security and privacy controls. The HITRUST Risk-based, 2-year (r2) Validated Assessment *(formerly named the HITRUST CSF Validated Assessment)* demonstrates that an organization is taking the most proactive approach to data protection and information risk mitigation. The r2 is globally recognized as a high-level validation that an organization successfully manages risk by meeting and exceeding industry-defined and accepted information security requirements.

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 quality review, and consistency of oversight. For organizations sharing sensitive information, handling high volumes of data, or facing challenging regulatory requirements, a properly scoped r2 Assessment ensures that control requirements are effective and compliant. The r2 offers flexible, tailorable, risk-based control selection to meet the most stringent needs.

r2 At-A-Glance Overview

	HITRUST Risk-based, 2-year (r2) Validated Assessment
Description	**Validated Assessment + Risk-based Certification**
Purpose (Use Case)	Focuses on a comprehensive risk-based specification of controls suitable for most organizations with a rigorous approach to evaluation, which is suitable for high assurance requirements
Targeted Coverage	NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, AICPA TSC, PCI DSS, GDPR, and a full range of others
Number of Control Requirement Statements	2000+ based on Tailoring (360 average in scope of assessments)
Flexibility of Control Selection	Tailoring
Evaluation Approach	PRISMA 3×5 or 5×5: Control Maturity assessment against either 3 or 5 maturity levels
Level of Effort / Level of Assurance Conveyed	High
Certifiable Assessment	Yes, 2-year
Complementary Assessments	Readiness, Interim, Bridge
4th-Party-Performed Controls (Control Requirements Performed by Subservice Providers)	Included
Shares Assessment Results with Relying Parties through the HITRUST Results Distribution System™	Yes
Leverages HITRUST Assurance Intelligence Engine™ (AIE) to Prevent Omissions, Errors, or Fraud	Yes

The HITRUST Risk-based r2 Validated Assessment + Certification Delivers Reliable Information Security Assurances

By using a risk-based approach, the HITRUST r2 Assessment helps organizations address their most demanding security and data protection challenges. Earning an r2 Certification puts an organization into an elite group by showing that they meet key compliance requirements included across a wide range of industry standards and frameworks, as well as federal and state regulations. An r2 Assessment is also designed to identify control deficiencies so organizations can develop and implement efficient Corrective Action Plans (CAPs) to address those gaps.

During the assessment process, highly trained, independent HITRUST-Certified External Assessor firms use consistent methodologies to perform testing, scoring, and validation. After submission, the HITRUST Assurance Program™ establishes an unparalleled level of trust because each submitted assessment undergoes an exhaustive evaluation by HITRUST auditors. No other assessment uses such a rigorous, comprehensive, and centralized approach to deliver assurance results that are accurate, consistent, and reliable.

To Rely on Assurances, Stakeholders Need to Be Confident Results are Reliable

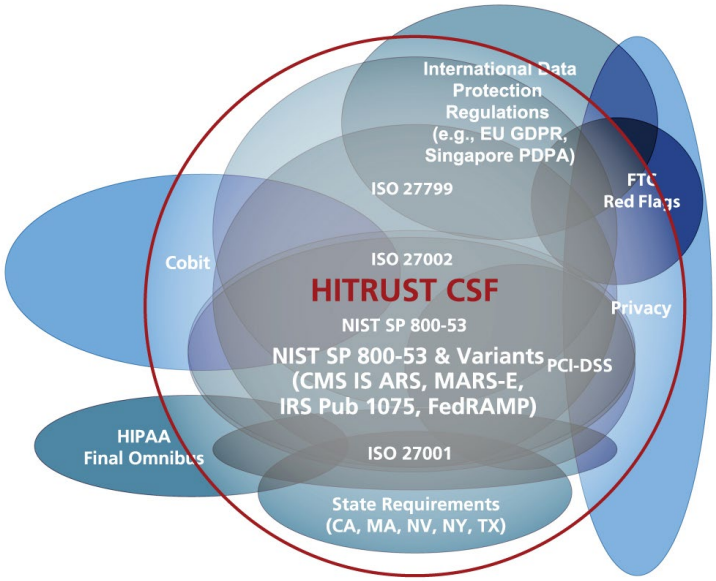
HITRUST Assessments Deliver: **TRANSPARENCY** + **ACCURACY** + **CONSISTENCY** + **INTEGRITY**

TRANSPARENCY. The publicly available HITRUST CSF framework and well-documented HITRUST Assurance Program offer full transparency regarding the assessment scope and review process.
ACCURACY. The HITRUST Approach™ relies on quantitative measurements to accurately evaluate, score, and assess the maturity of an organization's information risk management program.
CONSISTENCY. HITRUST External Assessors are trained and certified to consistently use HITRUST methodologies, and HITRUST has been used to perform hundreds of thousands of assessments.
INTEGRITY. HITRUST has rigorous requirements for External Assessors and our HITRUST Quality Assurance auditors so that business partners and other stakeholders can depend on the results.

r2 Assessments are Based on Comprehensive and Tailorable HITRUST CSF Control Requirements

The widely-adopted HITRUST CSF® is a single framework that includes more than 40 authoritative sources in a tailorable and flexible control library, which is harmonized and mapped to each source. Using the HITRUST MyCSF® platform, the r2 Assessment allows an organization to select whichever risk factors and compliance factors they require.

A properly scoped r2 Assessment offers coverage against: NIST SP 800-53, NIST CSF, ISO 27001, HIPAA, FedRAMP, FISMA, FTC Red Flags Rule Compliance, MARS-E Requirements, PCI DSS, CCPA, GDPR, AICPA Trust Services Criteria for Security, Confidentiality and Availability, plus more than 30 other industry-recognized frameworks, standards, and authoritative sources. While 75 prescribed controls within the HITRUST CSF framework are required for certification, organizations have the flexibility to scale and select other controls based on inherent risk factors and targeted authoritative sources.

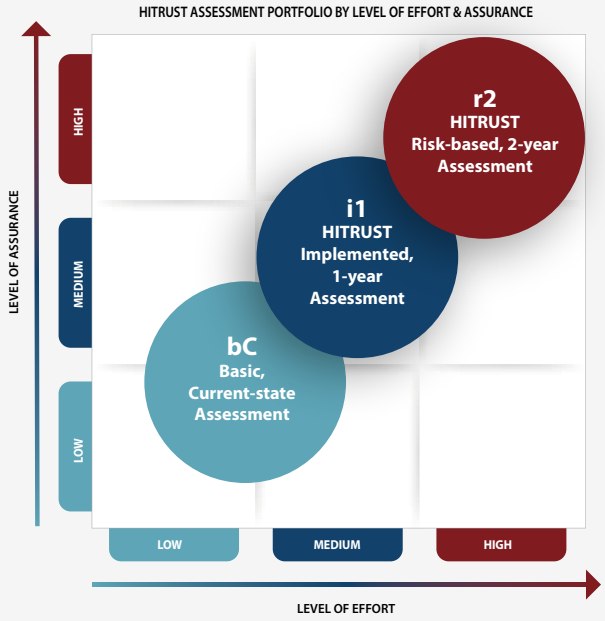


HITRUST Innovation Improves Quality, Efficiency, and User Experience

- The HITRUST CSF® framework provides prescriptive and granular control requirements and the HITRUST MyCSF® platform manages assessments efficiently and effectively
- Consistent and comprehensive assessment approach with proven assurance methodologies that deliver accurate results
- Offers *Assess Once, Report Many*™ benefits by meeting multiple requirements and minimizing the need for additional reports
- Supports HITRUST Control Inheritance, which saves time by importing results and scores from prior r2 Assessment(s)
- Uses the patent pending HITRUST Assurance Intelligence Engine (AIE) for analyzing and verifying assessment documentation to pinpoint oversights, errors, and inconsistencies so they can be fixed prior to submission
- Leverages the HITRUST Results Distribution System™ (RDS) online portal to share assurance results with relying parties through a PDF, web browser, and/or API so they can obtain, interpret, and analyze assessments more efficiently

How the r2 Fits into the Full HITRUST Assessment Portfolio

All HITRUST Assessments leverage a single framework, assessment platform, and assurance methodology. This approach ensures consistency and efficiency across the entire assessment portfolio.



HITRUST Risk-based, 2-year (r2) Validated Assessment is a tailorable assessment that focuses on comprehensive, prescriptive, risk-based controls specification and selection with a very rigorous approach to evaluation. These factors combine to ensure that the r2 consistently provides the highest level of assurance for organizations with the greatest risk exposure.

HITRUST Implemented, 1-year (i1) Validated Assessment delivers a relatively moderate level of assurance for information-sharing situations with lower risk thresholds. 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 evaluated (implementation only for an i1).

HITRUST Basic, Current-state (bC) Assessment is a verified self-assessment that provides a simpler approach to evaluation, which is suitable for scenarios requiring rapid or lower levels of assurance. Since the bC is a self-assessment, there is no scoping, scoring, or validation by External Assessors or the HITRUST Assurance and Quality teams, and no certification is offered.

Similarities and Differences Between the i1 and r2 Certifications

Similarities

- Both r2 and i1 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 + Certification can be performed for both
- Both require an Authorized HITRUST External Assessor organization to validate testing and evidence before submitting to HITRUST
- Both undergo full Quality Assurance (QA) by HITRUST
- Both use requirements included in the HITRUST CSF and both can use the HITRUST MyCSF SaaS best in class information risk management platform
- Both the r2 and i1Reports can be shared through the HITRUST Assessment XChange™

Differences

- An r2 Assessment requires more time and effort to complete than an i1 Assessment
- An r2 Certification is valid for two years, while an i1 Certification is valid for one year – consequently, no interim or bridge assessment is necessary for the i1
- 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 included in i1 Assessments considers only control Implementation
- Since an r2 Assessment can be tailored to include up to 2000 control requirements, the r2 can be used to evaluate compliance with a wider range of regulations and authoritative sources than an i1
- While requirements considered in r2 Assessments can be tailored based on authoritative sources and the assessed entity's inherent risk factors, 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
- 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
- To assist covered entities and business associates in healthcare, the proprietary HITRUST MyCSF® Compliance and Reporting Pack for HIPAA automatically compiles evidence collected during an r2 Assessment. However, the HIPAA compliance pack is not available during an i1 Assessment

NIST

A separate NIST CSF Report is provided with the r2 Validated Assessment Report detailing an organization's compliance with NIST Cybersecurity Framework-related controls included in the HITRUST CSF framework, but is not part of an i1.

For HIPAA compliance, there are significant differences between r2 and i1 Assessments.

Providing demonstrable assurances showing compliance with HIPAA Security, Breach, and Privacy Rules requires a properly scoped r2 Validated Assessment. However, since the i1 Assessment meets more than 90% of the HIPAA Security Rule, it can serve healthcare organizations as part of a HIPAA-compliant program that meets Safe Harbor requirements and provides meaningful assurances to relying parties. Plus, there may be instances when an organization wants to evaluate progress and effort towards HIPAA compliance — and an i1 Assessment could be useful as an intermediate step towards an r2 Assessment.

Benefits of a HITRUST r2 Certification

- A HITRUST r2 Assessment + Certification is the gold standard in providing responsible assurances for risk management and compliance due to its rigorous, comprehensive, and effective approach
- Provides a comprehensive r2 Certification Report, which can reduce costs and effort compared to completing proprietary questionnaires, multiple assessments, and single-use assurance reports
- The HITRUST r2 will satisfy the most rigorous assurance needs of multiple internal and external stakeholders – *Assess Once, Report Many*™
- The HITRUST r2 provides a competitive advantage in strengthening existing business relationships and earning new partnerships – especially in situations with significant volumes of PII, ePHI, and other sensitive data that requires the highest levels of assurance
- The rigorous level of assurance shown by a HITRUST r2 Validated Assessment helps an organization show justification for a reduction in cyber insurance premiums
- The HITRUST r2 provides added peace-of-mind that an organization's data networks and IT assets are protected from intrusion and breaches

HITRUST Offers Several 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 includes 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.

HITRUST r2 Readiness, Interim, and Bridge Assessments

Readiness Assessment. Often used to prepare for a future r2 Validated Assessment + Certification. With oversight and governance by HITRUST, generates a standard report and compliance scorecard – and if needed, Corrective Action Plans (CAPs). Although HITRUST generates a report for Readiness Assessments, results are not validated, so they provide a limited level of assurance. The MyCSF assessment tool can streamline the process of scoping and tailoring an r2 Readiness Assessment. MyCSF is available for 90-day use as part of a HITRUST Readiness Assessment Report or as an annual subscription, which allows data to be retained for later use.

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.

For More Information about the Risk-based, 2-year (r2) Validated Assessment:

Contact your HITRUST Product Specialist

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