

Why HITRUST Certifications are Broadly Accepted and Considered the Gold Standard



The Best Information Protection Assurances Available

In the current global ecosystem of ever-evolving cyber threats, vendors need to efficiently provide assurances that they have effective security and privacy controls in place to comply with a multitude of regulations. On the other side of the equation, customers must have confidence they are obtaining adequate security and privacy control assurances from their trading partners and vendors without overly burdening these entities with additional assessments and costs.

As the market-leading security, privacy, and compliance assessment, HITRUST Certifications demonstrate that an organization is taking the most proactive approach to data protection and information risk mitigation.

HITRUST Certifications are globally-recognized as a validation that information security and privacy controls are effective and compliant with various regulations. HITRUST Certifications are considered the gold standard in the industry because of the comprehensiveness and applicability of the control requirements, depth of the assurance process, and level of oversight that ensures accuracy. Individually, each element exceeds most other programs, and collectively they make HITRUST Certifications the most comprehensive, transparent, consistent, and highest quality assessments available.

The Gold Standard You Can Trust and Rely On

HITRUST Certification serves as an organization's passport to providing assurances to internal stakeholders, customers, regulators, and others requiring information assurances – including cybersecurity insurers. Many other assessment reports lack transparency regarding specific requirements, what was assessed, the review process, and quality checks. It is no wonder that thousands of organizations, globally and across all industries accept, and in many cases require, a HITRUST Certification from vendors and third-party service providers for security and privacy assurances.

Leveraging HITRUST Certifications can result in significant reductions in risk and the level of effort required compared to relying on proprietary questionnaires or other assurance reports without the same level of transparency, accuracy, integrity, or 'Rely-Ability' offered by a HITRUST Certification.

Given the breadth of control coverage and the comprehensive nature of HITRUST's assurance requirements, a HITRUST Certification report provides assurances relating to a variety of standards and regulations, which can reduce costs and effort compared to completing proprietary vendor questionnaires, multiple assessments, single-use assurances, and other compliance reports.



Reasons Why Leading Organizations Rely On HITRUST

- 1 A HITRUST Certification is the **gold standard** in providing assurances of risk management and compliance due to its rigorous, comprehensive, and effective approach.
- 2 HITRUST Certifications are the preferred approach for demonstrating and communicating the effectiveness of privacy and security controls as the **universal passport for assurances** with world-wide recognition and acceptance.
- 3 The HITRUST CSF, the foundation of HITRUST Assessments, integrates and harmonizes **dozens of authoritative sources** and incorporates almost 2,000 available controls into one certifiable framework.
- 4 HITRUST **continually updates** its methodologies, programs, and solutions to **stay ahead** of evolving cyber threats, changing regulations, and increasingly complex IT infrastructures.
- 5 HITRUST **standardizes the approach to risk management** while being transparent about its methodologies. Risk questionnaires vary widely, do not provide adequate transparency, and are not the most accurate assessment of risk because they merely *check-a-box* and often do not provide a true measure of information protection program effectiveness.
- 6 Each assessment submitted by a HITRUST Authorized External Assessor undergoes nearly 150 automated quality checks to identify and address assessment errors and omissions. In addition, each HITRUST Assessment undergoes at least 5 levels of independent and objective quality review by Assurance Analysts within HITRUST's Assurance team for validation. **No other methodology uses such a rigorous, comprehensive, and centralized approach** to deliver assurance reports that are accurate, consistent, and reliable—an attribute that is critical for making risk-based decisions across an organization.

Since 2007, HITRUST has been architecting and implementing a comprehensive and fully integrated approach to information risk management and compliance assessment and reporting that provides a level of transparency, scalability, consistency, accuracy, integrity, and efficiency simply not obtainable through other approaches and/or assurance report mechanisms. HITRUST's unique and comprehensive approach to information risk management and compliance—The HITRUST Approach—addresses all of these criteria to provide the most robust assurance option available.

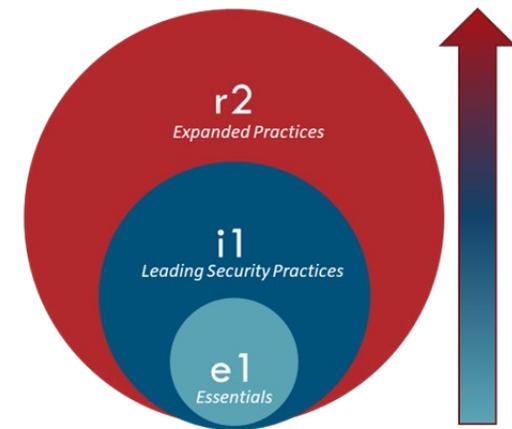
HITRUST CSF®

A HITRUST Validated Assessment + Certification leverages the HITRUST CSF, which is a comprehensive, scalable, and risk-based framework that integrates dozens of privacy and security regulations and standards to ensure complete coverage of controls. Includes 2000+ control requirements in a fully tailorable and flexible control library, which is harmonized and mapped to each authoritative source.

Assessment Portfolio Designed to Support an Efficient Path to Certification

3 HITRUST Certification Options

For varying levels of budget, resources, and risk



Control Nesting Facilitates a Seamless, Efficient, and Progressive Assessment Journey to Demonstrate Growing Security Capabilities

HITRUST Essentials, 1-Year (e1) Validated Assessment + Certification

Provides entry-level assurance focused on the most critical information security controls and demonstrates that essential cybersecurity hygiene is in place.

HITRUST Implemented, 1-Year (i1) Validated Assessment + Certification

Provides a moderate level of assurance that addresses cybersecurity leading practices and a broader range of active cyber threats than the e1 Assessment.

HITRUST Risk-based, 2-Year (r2) Validated Assessment + Certification

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.

The Rigorous HITRUST Assessment and Validation Process Assures Complete Rely-Ability™

TRANSPARENCY

Transparency is needed for internal and external stakeholders to understand the framework your organization uses to satisfy compliance objectives. The framework should be publicly available, widely adopted, and well-understood **so that report recipients understand how the controls were selected, evaluated, and scored.**

- HITRUST CSF® control framework is prescriptive, publicly available, widely adopted; and updates are documented extensively in each release.
- HITRUST Assurance Program™ includes a robust assessment approach, control maturity and scoring methodologies, and related assurance requirements, which are clearly articulated in publicly available guidance.

ACCURACY

Many other frameworks are qualitative, judgment-based, and devoid of any quantitative measurements. By contrast:

- **HITRUST precisely evaluates and scores security and privacy controls** while identifying deficiencies, gaps, and weaknesses.
- **HITRUST uses a five-point PRISMA-based maturity model and evaluates each of the maturity levels** against a five-point compliance scale, which ranges from non-compliant to fully compliant.
 1. Policy – Are management's expectations clearly laid out in written policies?
 2. Procedure – Are operational aspects of the control defined and written into procedures?
 3. Implemented – Is each control in place? Is it operating as expected?
 4. Measured – Is there a mechanism in place that informs the organization when a control is not performing effectively?
 5. Managed – Is the organization addressing risks as they are identified?

Note: Only the HITRUST r2 Assessment evaluates all five maturity levels. When a less rigorous level of assurance is needed, the HITRUST e1 and i1 Assessments only evaluate Implemented to reduce effort.

CONSISTENCY

When frameworks are vague, subjective, or free of maturity levels and scoring methodologies, it becomes difficult to gauge an organization's posture against that of another framework or even an industry baseline. This problem is compounded when assessment activities are not subject to quality and integrity reviews by an independent third-party assessor.

- **HITRUST Authorized External Assessors are trained and certified to use HITRUST's assessment and assurance methodologies** as part of the certification process to ensure each control is documented, analyzed, tested, and validated.
- **The HITRUST Quality Assurance team reviews 100% of assessments** that are submitted for certification.

INTEGRITY

Simply put, the integrity of your assessment results and assurances to internal and external stakeholders depends upon an audit and validation process during which trained external assessors evaluate your control requirements one by one and say things like: "Prove to me you're doing this," or "Show me where it's documented."

- **HITRUST has rigorous certification requirements for External Assessors**, who have the important role of testing and validating security controls and have vast experience in IT compliance and auditing. They must complete a training course and pass an exam to become certified, then maintain their certification with annual refresher courses. This is another way that HITRUST ensures the assessment and certification process is Rely-Able.
- Submitted assessments undergo over **150 automated quality checks** using the patent pending HITRUST Assurance Intelligence Engine to identify and address errors and omissions, and then another **5 levels of independent and objective quality assurance reviews** by HITRUST assurance auditors.



Value of a HITRUST Certification

HITRUST Certification demonstrates that your organization is taking the most proactive approach to cybersecurity, data protection, and risk mitigation.

- 1 Market Differentiator**
Delivers a competitive advantage to expand existing partnerships and earn new business – including speeding and strengthening RFP responses.
- 2 Less Risk Exposure**
Offers added peace-of-mind that data networks and IT assets are protected from intrusion and breaches.
- 3 Adds Confidence**
Demonstrates that your organization has a strong cybersecurity program in-place.
- 4 Saves Effort**
Provides a comprehensive Certification Report, which can reduce time and cost compared to completing proprietary questionnaires, multiple assessments, and single-use assurance reports.
- 5 Increases Cyber Awareness**
Establishes a proactive culture across an organization indicating a collaborative team commitment to improving information security and privacy.
- 6 Cyber Insurance Advantages**
Shows justification for more favorable cyber insurance premiums.

HITRUST Certification serves as the **preferred and often required assurance** report for many organizations and multiple stakeholders in a wide range of industries.

Learn more about HITRUST Certification at [HITRUSTAlliance.net](https://www.HITRUSTAlliance.net)