How does HITRUST Certification Compare to Alternative Cybersecurity Assessments?

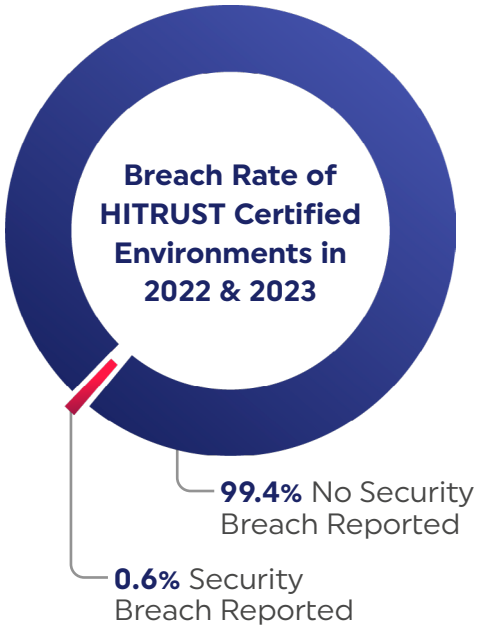
Evaluating an organization's cybersecurity and data security posture is critical to building professional trust, whether you're a customer, vendor, or service provider. Organizations can take various approaches in assessing trustworthiness. Examples include using custom questionnaires, well-established attestations, or conducting audits. All approaches are not equal, and it is important to understand the distinctions.

HITRUST certification uses consistent, quantitative, systematic methodologies that deliver an objective, measurable approach to evaluating organizations. Here are key points to help you make an informed decision.

What is HITRUST?

Since 2007, HITRUST has championed programs that safeguard sensitive information and manage cybersecurity risk. HITRUST is used globally, across industries, and throughout the third-party supply chain. As the leading provider of cybersecurity and information security assurances, HITRUST's programs and frameworks represent the highest standard in information risk, security, and compliance management.

HITRUST certifications are a result of prescriptive, relevant, threat-adaptive control requirements, proven through a reliable implementation, verification, and review methodology. Organizations who earn HITRUST certification have demonstrated their strength and risk maturity through a thorough, rigorous process.



Why is HITRUST the Best Approach to Assurance?

HITRUST is the only assurance program that **measures, monitors, and can precisely quantify** information security events.

- **Less than 1%** of HITRUST-certified organizations experienced a cybersecurity breach in 2022-2023, compared to industry-reported double-digit breach rates.
- HITRUST is the only assurance program proven to **materially and measurably reduce cyber risk** and the only program able to provide a benchmark due to its consistency and integrity.
- **100% of addressable Techniques, Tactics, and Procedures (TTPs)** included in the MITRE ATT&CK Framework are covered in the HITRUST Comprehensive Security Framework (CSF ®).

Organizations that choose HITRUST certification have committed to the most comprehensive, relevant, and reliable cybersecurity practices available. This commitment significantly reduces their risk of data breaches and strengthens their overall security posture.

HITRUST

The HITRUST CSF Comprehensive Framework

The HITRUST Assessment and Certification Program is built on the HITRUST CSF, which harmonizes and aligns over 50 authoritative sources, regulations, and best practices, including HIPAA, ISO, and NIST.

- Addresses the need for an actionable, common, and comprehensive framework.
- Defines control requirements in highly prescriptive terms, ensuring environments are **evaluated, validated, and documented** accurately, consistently, and transparently.
- Uses quantitative measurements, not subjective opinions, for certification.

Proactive and Threat-Adaptive

HITRUST certification is **cyber threat-adaptive**. That means that the HITRUST framework is regularly updated to include controls that evolve to address new cyber risks while remaining harmonized with established frameworks, ensuring both security and compliance. This approach helps signal that organizations using HITRUST are taking the most proactive approach to data protection and cybersecurity.

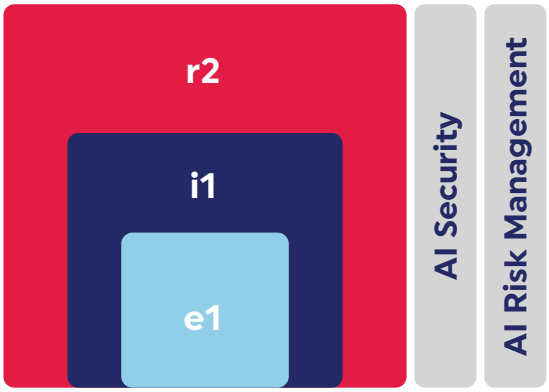
- Organizations seeking recertification on an annual or bi-annual basis must demonstrate compliance against the most current security controls, which are regularly tested and updated against the latest threat intelligence.
- The HITRUST CSF is updated at least twice a year to incorporate new authoritative sources and respond to emerging threats, such as those introduced by AI.
- HITRUST certification is only valid for 1-2 years, encouraging a long-term, continuous improvement approach to security.
- Corrective Action Plans (CAPs) are provided during certification to further enhance cybersecurity practices, address any gaps, or define areas for improvement and 92% of CAPs have historically been resolved within 12 months.

The HITRUST Assessment Portfolio

r2 HITRUST 2-year Assessment - ***250+ controls*** The r2 is the most comprehensive and robust HITRUST assessment. It is designed for organizations that need to demonstrate expanded regulatory compliance with HIPAA, NIST, and other authoritative cybersecurity sources, and for those that require expanded tailoring of controls based on identified risk factors.

i1 HITRUST, 1-Year Assessment - ***182 controls*** The i1 is ideal for established security programs.
It allows organizations to demonstrate leading security practices and comprehensive assurance. It can also be used as a first step toward attaining an r2 certification.

e1 HITRUST, 1-Year Assessment - ***44 controls*** The e1 certification allows organizations to demonstrate that they meet foundational security practices. It is often best for startups and organizations with lower inherent risks or complexity. It can also be used as a first step toward attaining i1 or r2 certifications.



The AI Certification

The AI Certification provides AI platform and service providers with practical controls to secure AI technologies. It can be added to an e1, i1, or r2 to support shared responsibility and to streamline compliance across multiple requirements.

AI Risk Management Assessment

The AI Risk Management Assessment is not a certification. It provides a means to effectively evaluate your AI risk management program, identify your potential gaps, and create action plans to continuously improve your risk management posture.

HITRUST