Selecting the Right Cybersecurity Assurance Mechanism

Business leaders face a high-stakes question: which cybersecurity assurance approach can you trust to reduce risk — and prove it?

This eBook provides a clear-eyed comparison of the four most well-known assurance mechanisms — NIST SP 800-53, ISO 27001, SOC 2, and HITRUST and dives deeper into exploring SOC 2 vs. HITRUST.

Learn why organizations that adopt HITRUST not only meet compliance requirements, but also achieve stronger risk reduction, greater scalability, and measurable results.

HITRUST®

Cyber Threats Could Grind Your Business to a Halt

Cyber threats, data breaches, and ransomware attacks are happening everywhere. Every organization, big or small, is vulnerable. The breakneck pace of evolution in technology means the threat landscape is evolving just as quickly. Cybercriminals are not just targeting your organization. They know they can often inflict the greatest harm by going after your vendors, whose cybersecurity rigor may not be as strong as yours.

While attacks remain widespread, organizations stand to lose more than control of sensitive data. Just as often, ransomware attacks leave organizations' supply chains paralyzed, causing massive disruptions. Today, organizations have to worry about business continuity as well as the loss of data privacy and integrity. Small and medium businesses can be common targets, and they can be even more at risk if they provide goods and services to larger, more complex organizations. Bad actors often assume that these organizations are easy pickings, expecting them to scrimp on security practices due to a lack of budget or competing business priorities. This can make them vulnerable. And those vulnerabilities can impact others in their supply chain and overall ecosystem.

When their data is compromised, organizations may lose much more than they saved by opting for less comprehensive information security safeguards. The extended damage can be nearly incalculable.

In 2024, the FBI's Internet Crime Complaint Center received

859,532
cyber complaints

$16 billion
reported losses

A 33% increase compared to 2023

Organizations are worried about the rising number of cyberattacks. They are asking themselves how best to safeguard their sensitive data and protect their supply chain. They are losing trust in the old ways of doing things and looking for better solutions. They are demanding assurances that their data and their customers' data are safe all along the information supply chain.

Verizon's 2025 Data Breach Investigations Report analyzed over 22,000 security incidents and 12,195 confirmed data breaches in 2024. Notably, exploitation of vulnerabilities as an initial attack vector increased by 34%, now accounting for 20% of breaches. Furthermore, ransomware attacks rose by 37% since last year and are now present in 44% of breaches. These findings underscore the critical need for organizations to adopt comprehensive and adaptive security measures.

The big question remains — how do you earn the trust of your customers and stakeholders when it comes to protecting their data?

44%

of breaches in 2024 involved ransomware

Three Key Assessment Parameters

Organizations need robust assurances to reduce risk and demonstrate the maturity of their security postures. The following three parameters are crucial in identifying effective, trusted assurance.

Relevant Controls

Controls that are **highly prescriptive and detailed** leave little room for interpretation. They must be **threat adaptive** to reflect the evolving threat landscape and structured to **align with industry standards** while enabling seamless progression to more robust assessments.

These relevant controls give specific, responsive, and harmonized guidelines for better security.

Reliable Assurances

Assurances become reliable when they are **third-party validated**, ensuring credibility through independent verification. They must also maintain **centralized quality review** and employ **standardized scoring and reporting** methods across all assessments.

This unified approach guarantees consistent, objective, and authoritative assurance across organizations and industries.

Proven Results

Assurance mechanisms must demonstrate **measurable and repeatable impact**, produce **strong mitigation outcomes** for managing security and privacy risks, and support **continuous improvement** to help organizations remain resilient and responsive.

These proven outcomes build trust and deliver ongoing, tangible improvements in compliance and cybersecurity performance.

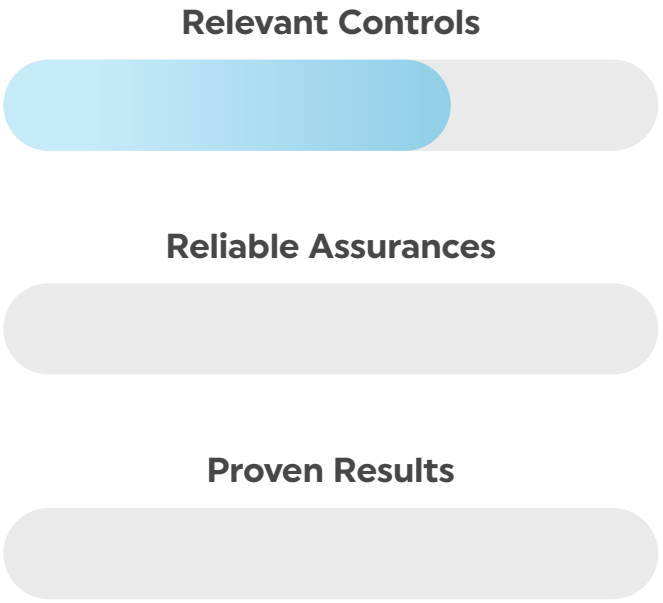
Types of Assurance Mechanisms

NIST SP 800-53 Assessment

NIST SP 800-53 offers one of the most extensive sets of security and privacy controls available, tailored for use in federal systems and critical infrastructure. It serves as a foundational control library for government entities and contractors, enabling structured risk mitigation in complex and high-threat environments.

Despite its breadth, NIST SP 800-53 lacks a formal certification program, maturity scoring, or centralized reporting. It does not adapt its controls in response to the evolving cyber threat landscape, making it slower to address emerging risks. The most recent update to NIST SP 800-53 occurred in November 2023.

Additionally, implementation requires significant effort, and there's no native support for commercial regulatory needs. This makes it less accessible and less practical for non-government organizations seeking actionable security certification.

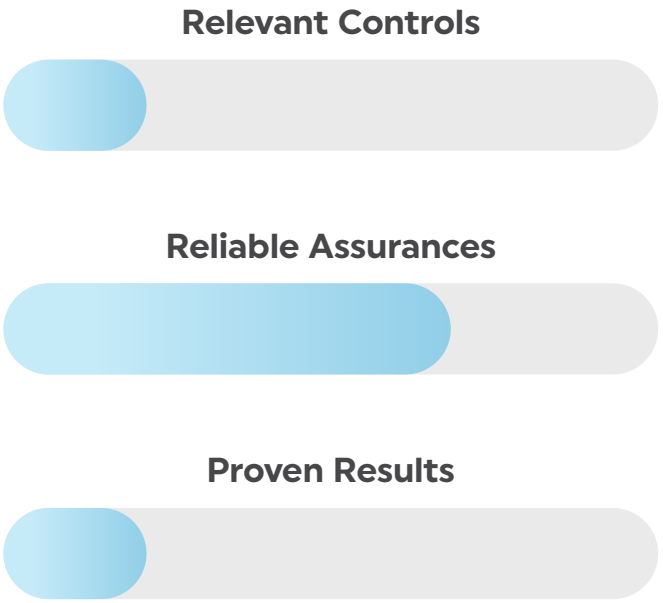


ISO 27001 Assessment

ISO 27001 delivers a globally respected standard for establishing, implementing, and maintaining an Information Security Management System (ISMS). Its flexible, risk-based approach allows organizations to tailor controls to their unique business context, making it highly suitable for companies seeking strategic, long-term information security governance aligned with international best practices.

While ISO 27001 offers broad strategic value, it lacks detailed control guidance, formal maturity scoring, and direct regulatory mappings. Like NIST SP 800-53, ISO is not designed to adapt dynamically to changes in the cyber threat landscape, limiting its ability to address emerging risks.

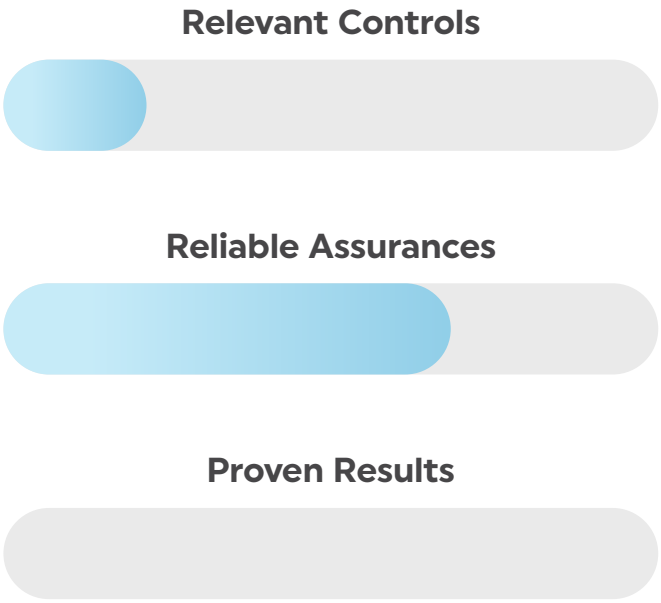
ISO/IEC 27001 was last updated in 2024. This makes it less effective than other standards for organizations needing granular, auditable evidence of control performance.



SOC 2 Attestation

SOC 2 provides third-party assurance over key operational controls through an audit framework built around Trust Services Criteria. It's particularly valuable for service providers, SaaS companies, and tech firms needing to demonstrate security, availability, or privacy controls to customers and partners in a flexible, non-prescriptive format.

SOC 2 lacks standardized control requirements, a formal maturity model, and built-in regulatory alignment. Assessment quality varies by auditor, and the binary reporting format limits transparency. This means it offers less consistency and assurance for organizations operating in highly regulated or risk-sensitive environments.

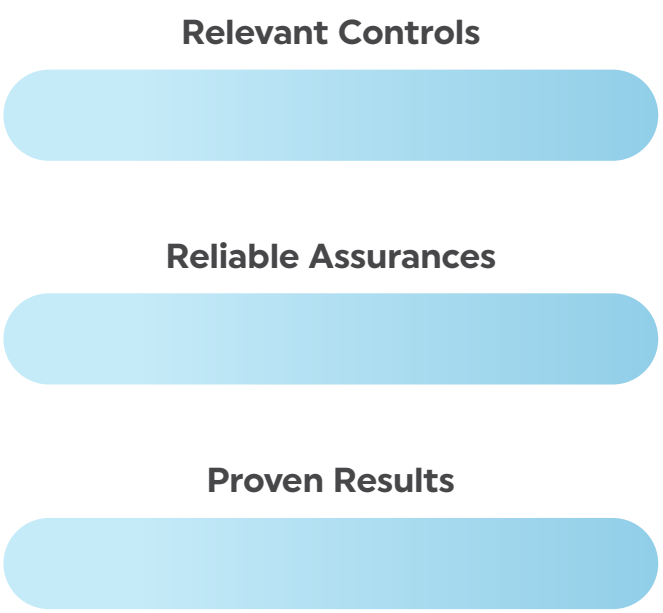


HITRUST Validated Assessment

HITRUST is the leader in cybersecurity assurance, offering certification programs for the application and validation of security, privacy, and AI controls. It is the only assurance mechanism proven to mitigate risk. HITRUST harmonizes more than 60 authoritative sources and makes them available through its comprehensive HITRUST CSF framework. The framework is updated regularly, with the most recent version being released in April 2025, making it relevant and cyber threat adaptive.

Working against this framework allows organizations to evaluate their risk maturity, identify potential gaps, and adopt enhanced security practices. HITRUST is built to counter modern cyber challenges and assessments.

With HITRUST certification, organizations can demonstrate their compliance with regulatory standards and security best practices using a globally recognized standard.



Choosing the Right Assurance

Assurance Mechanism Comparison		HITRUST	ISO 27001	NIST 800-53	SOC 2
Relevant Controls	Highly Prescriptive	✓	✗	✓	✗
	Threat-Adaptive	✓	✗	✗	✗
	Complete Certification Portfolio	✓	✗	✗	✗
	Aligned to Industry Standards	✓	✗	✓	✗
	Structured for Validation	✓	✓	✓	✓
Reliable Assurances	3rd-Party Validated	✓	✓	✗	✗
	Centralized QA	✓	✗	✗	✗
	Standardized Scoring	✓	✗	✗	✓
	Consistent Reporting	✓	✓	✗	✓
	Evidence-Based Testing & Validation	✓	✓	✗	✓
Proven Results	Repeatable, Measurable Results	✓	✗	✗	✗
	Proven Mitigation Outcomes	✓	✓	✗	✗
	Continuous Improvement	✓	✗	✗	✗
	Standardized Data Reporting	✓	✗	✗	✗
	Structured Corrective Action Plan Model	✓	✗	✗	✗

SOC 2 vs. HITRUST

While NIST, ISO, SOC 2, and HITRUST are all well-established assurance mechanisms, they differ significantly in purpose, implementation, and applicability. HITRUST and SOC 2 are uniquely positioned and are commonly adopted and accepted. As organizations often weigh these two options directly when selecting a path for security assurance, let's compare them to help you make informed, strategic decisions.

SOC 2 is an attestation, while HITRUST is a certification.

It is a common misconception that SOC 2 is a certification. It is an attestation report containing an opinion issued by a CPA firm. The report consists of an auditor's opinion on the suitability of the design and operating effectiveness of controls against specific criteria.

On the other hand, HITRUST is a trusted certification based on a well-documented framework of authoritative sources, offering reliable assurances and transparency.

SOC 2 is limited, while HITRUST is comprehensive.

The scope of SOC 2 is limited to the controls the organization selects. It often ignores important control areas essential for a comprehensive security program. For instance, SOC 2 may lack controls related to email security and Third-Party Risk Management (TPRM) programs.

The HITRUST CSF is the framework of all frameworks with highly prescriptive controls. HITRUST CSF v11.4 harmonizes 60+ authoritative sources so HITRUST customers can align with major, relevant cybersecurity frameworks by earning HITRUST certification. The HITRUST framework is threat adaptive and addresses 100% of the known Tactics, Techniques, and Procedures (TTPs) that can be mitigated.

SOC 2 is subjective, while HITRUST is formula-based.

Part of the SOC 2 reports are based on auditors' opinions. The organization's management owns most of the report and is responsible for selecting the controls. This makes the control selection in SOC 2 subjective.

HITRUST maintains accuracy in its assurance mechanism with a standardized, centralized scoring system. All HITRUST validated assessments are third-party verified and thoroughly reviewed for quality.

SOC 2 results are unclear, while HITRUST results are proven.

There is no known data proving the effectiveness of SOC 2 reports. The AICPA decentralizes the issuing of SOC 2 reports.

Only HITRUST delivers quantifiable proof that its certifications work, making them trustworthy. Organizations with HITRUST certifications reported a 0.59% incident rate in 2024 as per the HITRUST 2025 Trust Report. This means HITRUST results in actual risk reduction, as 99.41% of HITRUST-certified environments remained breach-free. Repeat HITRUST customers also saw continuous improvement and up to 54% fewer corrective actions.

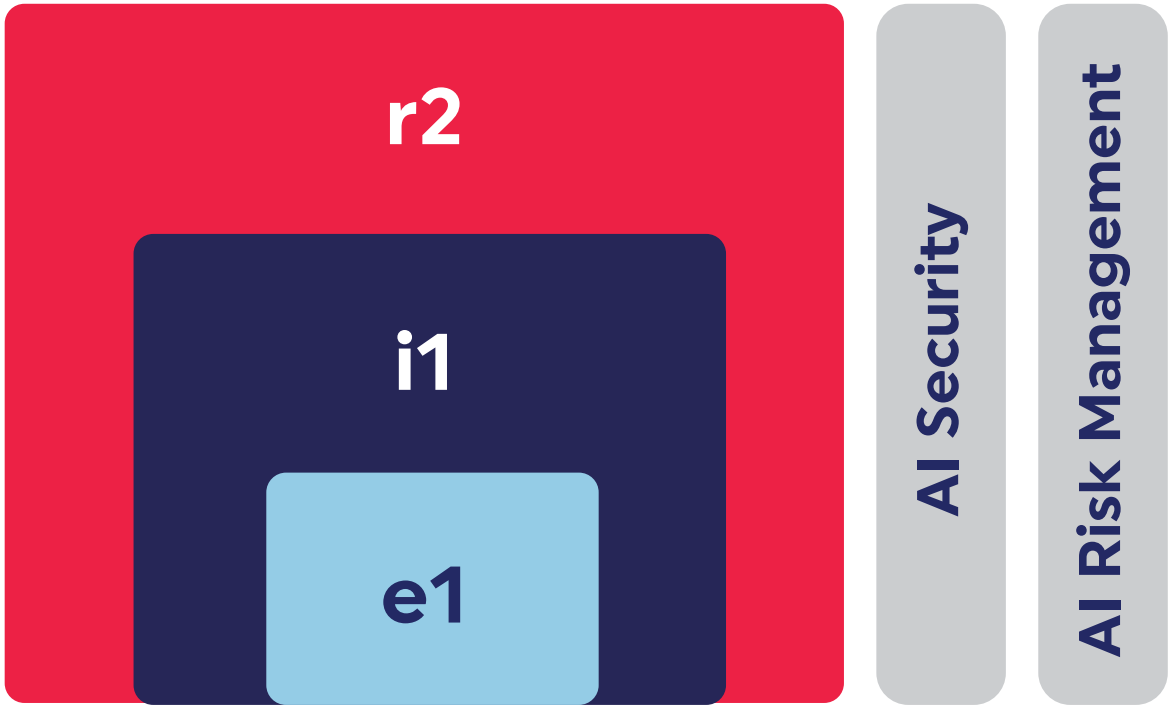
Benefits of HITRUST

- **HITRUST offers three core cybersecurity assessments and certifications.**
  HITRUST offers organizations the opportunity to choose among three certification types based on their risk profile and risk maturity. It can also serve as a foundation to get started and grow security practices by achieving consecutively higher assurances.
- **HITRUST controls can be mapped to and inherited from other sources.**
  Organizations can present their HITRUST assessment results in the context of specific compliance standards like HIPAA, PHIPA, or AI risk management, providing clear mappings between HITRUST controls and authoritative source requirements. Additionally, its Shared Responsibility and Inheritance Program allows organizations to inherit controls from previous assessments of vendors and cloud service providers.
- **HITRUST remains cyber threat adaptive to mitigate risk effectively.**
  HITRUST uses a comprehensive and continuous process to identify threats, align mitigations that counter ongoing and new threats, and position the organization to respond effectively. The HITRUST CSF is regularly reviewed and updated as necessary to respond to the constantly shifting threat landscape.

HITRUST Assessments and Certifications

The HITRUST assessment portfolio offers three core security certification options based on the organization's size, needs, and risk profile.

Because all three certifications are built on a common framework, the HITRUST approach is both traversable and tailorable. Organizations can apply work from their previous assessments to achieve more comprehensive certifications.



HITRUST e1

The e1 assessment and certification is ideal for startups and companies with limited risk profiles or less complexity. It allows for an entry-level validated assessment and certification based on 44 critical security controls. Organizations can also build upon these controls as a step toward attaining the more comprehensive i1 or r2 certifications.

HITRUST i1

The i1 assessment and certification is a good fit for organizations seeking moderate assurance to demonstrate leading security practices. The i1 offers a more comprehensive assurance than the e1, with 182 controls. Work done to attain an active i1 certification can be applied toward attaining an r2 certification.

HITRUST r2

The r2 assessment and certification is best suited for organizations that need to demonstrate regulatory compliance with authoritative sources like HIPAA, the NIST Cybersecurity Framework, and dozens of others that require expanded tailoring of controls based on other identified risk factors. It is the most comprehensive and robust HITRUST assessment.

In addition to e1, i1, and r2, HITRUST's two new AI security assurances empower organizations to embrace AI with confidence. HITRUST launched the industry-leading AI Security Assessment and Certification to seamlessly add AI assurance to any core certification, and the AI Risk Management Assessment tool so organizations can evaluate and continuously improve their AI risk management programs.

The HITRUST Advantage

HITRUST is the gold standard for organizations that need to streamline compliance, reduce risk, and build trust with customers and partners. By leveraging HITRUST's inheritance and centralized assurance processes, organizations save time, money, and resources while reducing the burden of responding to third-party security questionnaires. Earning a HITRUST certification sends a signal to regulators, customers, and stakeholders that they can trust the strength of your cybersecurity and data protection program.

Learn more about selecting the right assurance mechanism: https://hitrustalliance.net/assessments-and-certifications

HITRUST®