

**Select the Right Assurance Mechanism
to Earn the Highest Level of Trust**



HITRUST[®]

Cyber Threats are Everywhere

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. Attacks are widespread and rampant.

Organizations that hold sensitive information are common targets. Small and medium businesses often scrimp on security practices due to a lack of budget or other competing business priorities. This can make them vulnerable.

When their data is compromised, organizations may lose ten times more than what they saved by opting for less comprehensive information security safeguards.

In 2022, the FBI's Internet Crime Complaint Center (IC3) received

800,000+
cyber complaints

\$10.2+
billion reported
losses

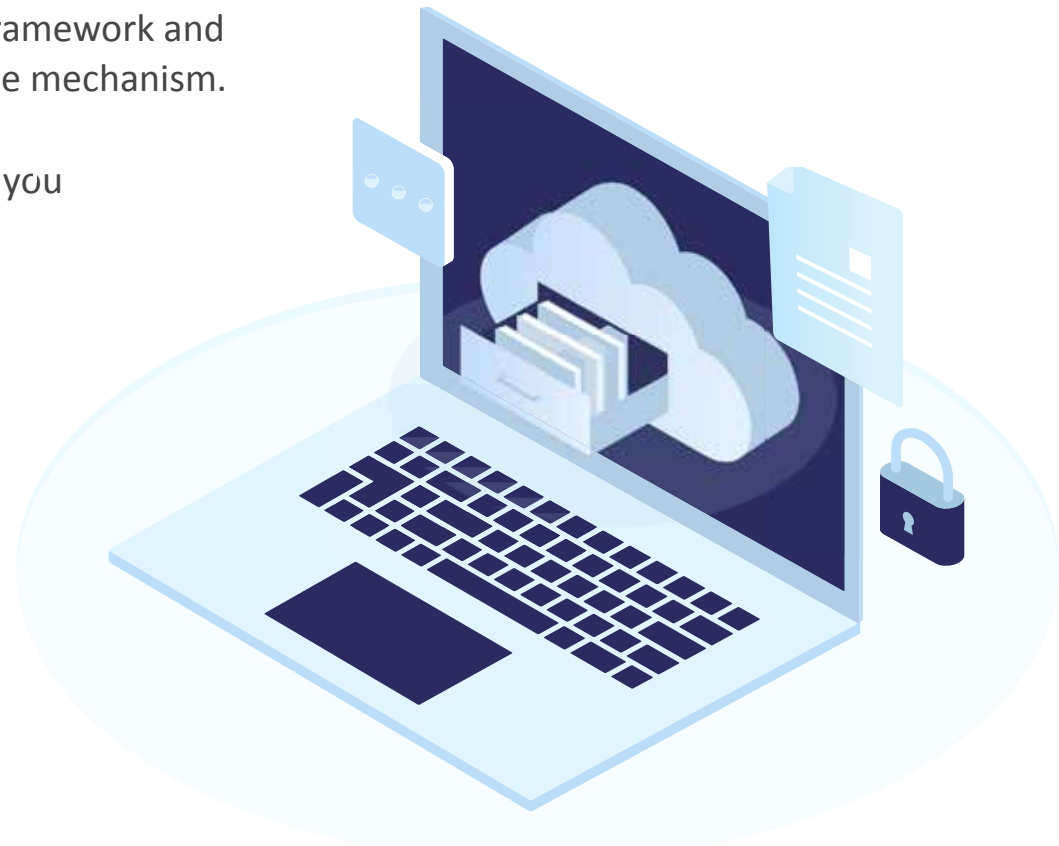
Healthcare, critical manufacturing, and government facilities were the top sectors affected.

Organizations are worried about the rising number of cyberattacks. They are asking themselves how best to safeguard their sensitive data. They are losing trust in their partners and vendors. They are demanding assurances that their data and their customers' data are safe all along the information supply chain.

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

The key is to adopt a respected information protection framework and demonstrate compliance with it using a reliable assurance mechanism.

But not all assurance mechanisms are the same. How do you pick the right one?



Four Key Assessment Parameters



Transparency

Transparency is essential for stakeholders to understand the framework and ensure it meets their risk and compliance objectives. The framework should be well-documented, published, and widely accepted.

- Look for clear guidelines to show how the controls were selected, evaluated, and scored.



Accuracy

Several frameworks and assurance programs are qualitative. They are based solely on the judgment of the assessors. However, the best assurance mechanisms ensure accuracy by being objective, reliable, and based on quantitative measurements.

- Check if the assurance mechanism is sourced from authoritative sources.



Consistency

Consistency is achieved through clarity of requirements that demonstrate maturity and scoring methodologies. When frameworks are vague, it becomes tough to understand an organization's maturity against that of other companies, another framework, or an industry baseline.

Similar standards and checklists across different organizations and industries ensure consistency. This makes it more likely for an assurance program to become widely recognized, accepted, and trusted.

- Look for consistent standards across organizations.



Integrity

Integrity depends on the testing methodology and rigor behind the assurance mechanism. Are assessors measuring organizations' practices based on an established methodology, reviewed by an accredited body? Assessors should evaluate each control requirement, verify the proof of implementation, and collect supporting evidence.

Following appropriate processes ensures the results are accurate and unbiased, with no conflicts of interest between the assessor, the assessed entity, and the certification body.

- Check that appropriate processes are followed.

Types of Assurance Mechanisms

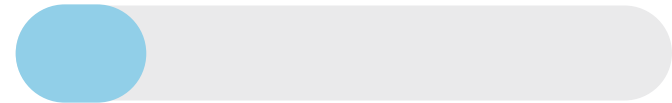
Cybersecurity Questionnaires

Cybersecurity questionnaires are one of the most common, traditionally-used assurances. These lists of complex and technical questions are distributed to collect information about the presence of security controls before an organization partners with a vendor. These are common in the request for proposal (RFP) vendor selection processes.

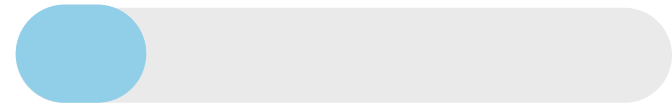
Organizations often create their own cybersecurity questionnaires. This lack of standardization makes it difficult and time-consuming for those answering the questions and those trying to gain some understanding from them.

While questionnaires may seem like an inexpensive approach to understanding inherent risk and risk maturity, they can be deceptively costly. Companies on both sides of the equation lose time and productivity completing and evaluating the information on questionnaires. As the information is only as good as the opinion of the person filling it out, questionnaires can be seen as semi-reliable attestations, at best.

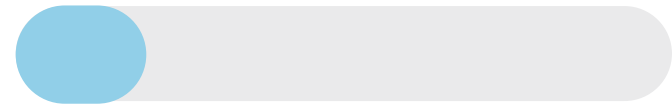
Transparency



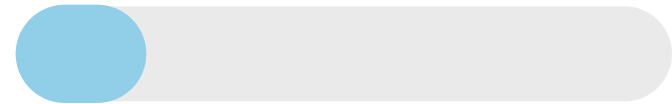
Accuracy



Consistency



Integrity



ISO 27001 Assessment

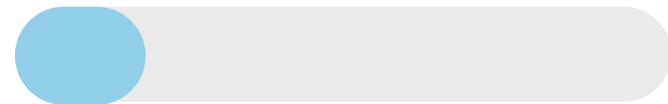
ISO 27001 is a standard that provides guidance for establishing, executing, and maintaining information security management systems. It offers assessment and certification. ISO 27001 focuses on safeguarding confidentiality, integrity, and availability of information.

The assurance mechanism of ISO 27001 is narrow in scope. It does not convey assurances over or compliance insights into any authoritative source except the ISO standard upon which it is built.

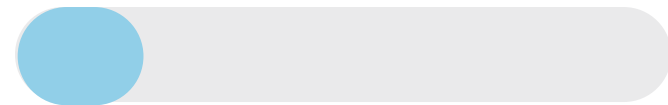
Transparency



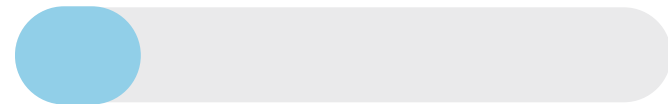
Accuracy



Consistency



Integrity



SOC 2 Attestation

Many organizations use SOC 2 reports to demonstrate that they take information security practices seriously. The SOC 2 was developed by the American Institute of Certified Public Accountants (AICPA). It allows organizations to attest to their measures and security controls. They can then have a CPA firm opine whether those attestations are accurately presented in the SOC 2 report.

A SOC 2 audit report only evaluates organizations against limited security controls they have selected to assess. This makes it highly variable, open to interpretation, not prescriptive, and difficult to compare.



HITRUST Validated Assessment

HITRUST is an information protection standards organization and certifying body. HITRUST harmonizes a number of authoritative sources and makes them available through its comprehensive, certifiable HITRUST CSF framework. The framework is updated regularly, 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. When they earn a HITRUST certification, organizations demonstrate their compliance with regulatory standards and security best practices using a globally recognized standard.

Transparency



Accuracy



Consistency



Integrity



SOC 2 vs. HITRUST®

Out of all the assurance mechanisms, SOC 2 and HITRUST are the two most commonly adopted and accepted. Evaluate them based on transparency, accuracy, consistency, and integrity to determine the best choice for your organization.



SOC 2 is an attestation, while HITRUST is a certification

It is a common misconception that SOC 2 is a certification. Instead, 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 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 integrity and accuracy in its assurance mechanism. HITRUST certification decisions are based on mathematical formulas, making them objective and quantitative and ensuring accuracy.



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, a SOC 2 may lack controls related to email security and Third-Party Risk Management (TPRM) programs.





HITRUST assessments are comprehensive, threat adaptive, and maintain consistency. They cover all 19 key domains, including endpoint protection, mobile device security, vulnerability management, and risk management.



SOC 2 reports are decentralized, while HITRUST results are centralized

As the AICPA chose to decentralize the issuing of reports, SOC 2 reports are only PDFs. It is not easy to extract data from PDFs and analyze it.

HITRUST Results Distribution System (RDS) offers a common portal for the electronic distribution of results. This makes it easy to share and analyze assessment results and ensure integrity throughout the process.

	PARAMETERS	SOC 2	HITRUST
	TRANSPARENCY	ATTESTATION	CERTIFICATION
	ACCURACY	SUBJECTIVE	FORMULA-BASED
	CONSISTENCY	LIMITED	COMPREHENSIVE
	INTEGRITY	DECENTRALIZED	CENTRALIZED

SOC 2

SOC 2 is an attestation report consisting of an auditor's opinion on the suitability of the design and operating effectiveness of controls against specific criteria.

- Reports partially based on auditor's opinions
- Organization's management responsible for selecting controls
- Subjective control selection
- Limited scope
- Often ignores control areas essential for a comprehensive security program
- Report may lack controls related to email security and TPRM programs
- Only available as PDFs
- Difficult to extract and analyze data

HITRUST

HITRUST is a trusted certification based on a framework of authoritative sources, offering reliable assurances.

- Maintains integrity and accuracy in assurance mechanism
- Decisions based on mathematical formulas
- Certification decisions are objective and quantitative
- Assessments maintain consistency and include all 19 key domains
- Domains include endpoint protection, mobile device security, vulnerability management, risk management
- Comprehensive and threat-adaptive assessments
- Electronic distribution of results via HITRUST RDS
- Results easily shared and analyzed

The Benefits of **HITRUST**

- **HITRUST offers three levels of assurance.**

HITRUST offers organizations the opportunity to choose among three certification levels 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.

- **The HITRUST CSF maps each control to multiple authoritative sources.**

These include HIPAA, ISO 27001, and GDPR. HITRUST can be mapped to SOC 2, too. The detailed mapping gives organizations a clear view of each control.

- **HITRUST is not a checklist.**

The time and effort that organizations and assessors put into the process yield reliable, consistent, and transparent results that are widely accepted and demonstrate security maturity.

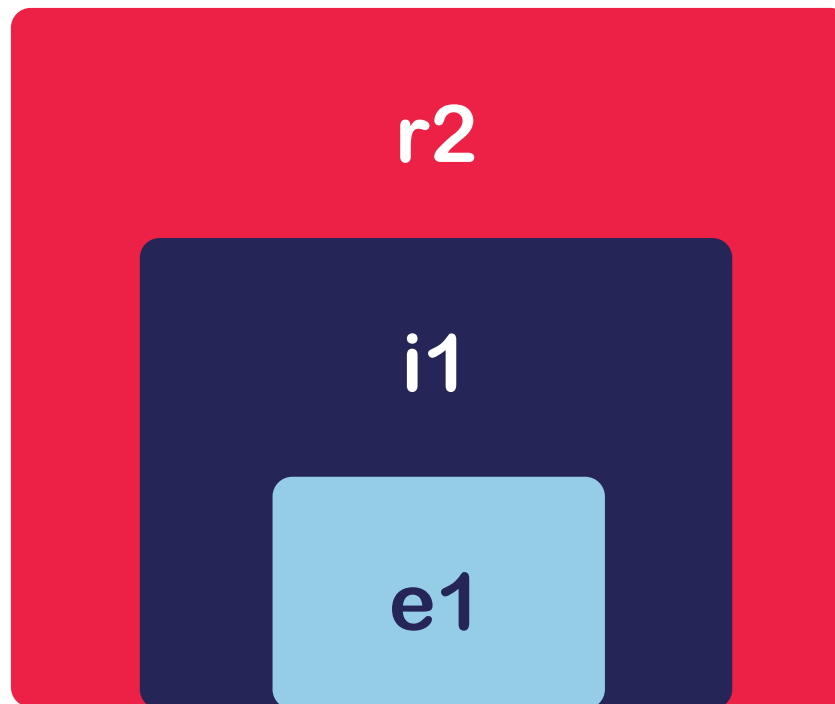
- **HITRUST streamlines companies' assurance journeys through inheritance.**

The HITRUST Shared Responsibility and Inheritance Program can help organizations save time, money, and resources by identifying inheritable controls from previous assessments.

Assessment Levels

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

Because all three certifications are built on a common framework, work from previous levels can be applied forward to more comprehensive certifications. Organizations working to attain certification can inherit existing controls, for example, from their certified cloud service providers.



HITRUST Risk-Based, 2-year (r2) Validated Assessment Expanded Practices

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

HITRUST Implemented, 1-year (i1) Validated Assessment Leading Security Practices

i1 is a good fit for organizations with robust information security programs already in place that are ready to demonstrate leading security practices. It could be good for mid-level organizations and offers a more comprehensive level of assurance than the e1, with more controls in scope. Work done to attain an active i1 certification can be applied toward attaining an r2.

HITRUST Essentials, 1-year (e1) Validated Assessment Foundational Cybersecurity

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

The **HITRUST** Advantage

HITRUST assessment gives you and your stakeholder organizations confidence that you have appropriate security practices in place. Organizations can trust you with their and their customers' sensitive data.

Because HITRUST certification is widely accepted, it can help streamline vendor selection and contracting processes. HITRUST helps your business stand out as a trustworthy choice.



HITRUST[®]



Learn more about selecting the right assurance mechanism to earn trust
here: info.hitrustalliance.net/hitrust-soc2-learn-more