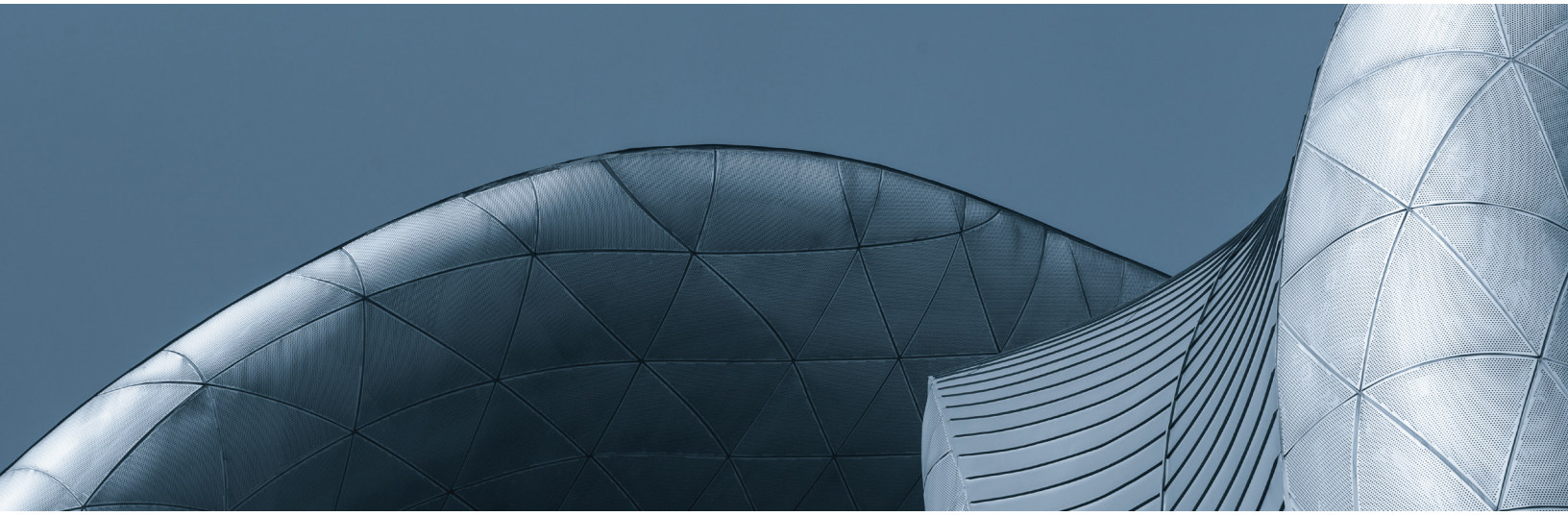
Enabling a Robust Cybersecurity Posture Through HITRUST Certification

HITRUST is a dynamic framework. It's a living, breathing organism, and evidence of that is in the dozens of authoritative sources utilized. Frequent updates to the CSF demonstrate that the HITRUST thought leadership is not just industry-centric, but industry-neutral. It's not just America-centric, but global. With the e1, i1, and the traditional r2 HITRUST certification options, organizations now have a credible, evidence rich framework to align their cyber and compliance strategy with their business drivers.

Uday Ali Pabrai
ecfirst | chief executive
MSEE, CISSP, HITRUST CCSFP

HITRUST® ecfirst TechTarget | xtelligent HEALTHCARE MEDIA



Introduction

It is happening everywhere, from ransomware attacks to phishing. Bad actors are transforming the current cyber threat landscape with ample opportunities to target victims and access sensitive data. In 2022 alone, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) received more than 800,000 complaints, with cyber victims collectively racking up more than $10.2 billion in losses.

IC3 received reports of ransomware attacks from organizations within 14 of the 16 designated critical infrastructure sectors. Healthcare, critical manufacturing, and government facilities were among the top sectors victimized by these forms of malware in 2022. Moreover, even organizations with strong internal security practices may be vulnerable to data breaches via a third-party vendor. For example, the majority of the top ten biggest healthcare data breaches reported to the United States Department of Health and Human Services (HHS) in 2022 stemmed from third-party vendors.

With these considerations in mind, it is more important than ever that organizations across all sectors take proactive steps to mitigate cyber risk. And the time to act is now. One important step forward is demonstrating compliance with industry-recognized certifications, an achievement that demonstrates an organization's commitment to safeguarding sensitive information through adherence to robust security measures and compliance protocols.

But not all certifications are created equal. With technology evolving rapidly and digital transformation taking hold across all industries, organizations require a dynamic, prescriptive, and risk-based certification program aimed at maintaining regulatory compliance, addressing security deficiencies, and adopting key risk management practices.

Choosing the right certification ensures the right controls are in place to protect sensitive data as cyber threats continue to grow while giving potential vendors strong assurances about the assessed organization's security maturity level.

HITRUST Over SOC 2

We all know the cyber threat landscape is ever-changing—threat actors constantly adjust their tactics and find new ways to target victims. The dynamic nature of current cyber threats requires an equally comprehensive assessment framework to evaluate security controls.

Reports such as the Systems Organization Controls 2 (SOC 2) can give organizations an idea of how they measure up to foundational cybersecurity controls. Developed by the American Institute of CPAs (AICPA), SOC 2 measures organizations against various security controls, delivering an audit report that speaks to the assessed organization's Data Availability, Security, Processing Integrity, Confidentiality, and Privacy.

A SOC 2 report can help organizations assess their security posture at a high level, providing insight into how well their internal systems protect sensitive data. New forms of assessments now offered by HITRUST can provide the same report as a SOC 2, but the HITRUST certification will take it many steps further. Rather than a certification, SOC 2 is an attestation about the trustworthiness of an organization's services.

> "I have security and risk conversations with my peers, the board, the executive team, the CTO and the CSO. The CSF is a great tool for getting everyone onto the same page."
>
> –Sr. Director of Security Strategy, financial technology services organization, WI

> "We can even provide a certification score to prove our level of maturity around the NIST cybersecurity framework; that's a feature that most other common frameworks do not provide."
>
> – VP of Information Security & Privacy, healthcare provider & insurer, PA

"From a regulatory standpoint, we're seeing a constant shift in adoption to go beyond a checkbox," said Scott Mattila, Chief Security Officer at Intraprise Health. "SOC 2 is defined by an organization. It is open to interpretation, and it is not prescriptive or threat adaptive. SOC 2 has its place, but it's foundational in a sense."

A SOC 2 report can provide organizations with key assurances about operational effectiveness and the security and privacy of data. However, HITRUST's assessment portfolio offers a more prescriptive and evidence-based journey beyond foundational security controls, emphasizing the difference between a certification and attestation.

"SOC 2 is not a certification, it is simply an attestation. You pass the SOC 2 and the public accounting firms will write a report to the executive leadership team stating that you met or did not meet certain requirements, and it is not based on risk. This is not a strong representation of a solid security program," said Ray Biondo, Executive Vice President and Chief Information Officer at BEYOND. "HITRUST has had more to do with bringing in best practice security into many organizations that never had it before. Having a HITRUST certification represents a strong security program through a third-party review. That is what really separates HITRUST from SOC 2."

"Approximately 40-50% of the prior year's revenue was due to our organization's HITRUST CSF Certification."

–CISO, technology organization, WI

In addition, the HITRUST CSF maps each control to multiple authoritative sources (e.g., HIPAA, GDPR, ISO 27001). The detailed mapping gives organizations a clear view into why each control is required. In fact, HITRUST can even be mapped to SOC 2.

"SOC 2 is an assertation/attestation. Anyone evaluating a company using a SOC 2 needs to review the criteria the company was evaluated against. For a HITRUST certification, the criteria are known and common for each type of certification," remarked Brian Golumbeck, Practice Director, Strategy and Risk Management at Optiv.

HITRUST's core values of consistency and transparency set it apart from other frameworks. Every assessment is evaluated for quality control by HITRUST itself. Additionally, all validated assessments flow through MyCSF—a centralized platform used by the assessed entity, the external assessor, and the HITRUST certification body.

What's more, the HITRUST CSF is updated multiple times per year to ensure that it stays relevant. New assessment options provided in the next section, allow assessed organizations to choose the path to HITRUST certification that aligns with their compliance needs.

"In the last year, more organizations, especially smaller organizations, have come to us with contractual requirements to get HITRUST certified," explained Brandon Weidemann, Manager, IT Risk Management at Meditology Services. "The benefit there is that the e1 and i1 now have been rolled out, making it much more attainable for those smaller organizations to achieve HITRUST certification."

External assessors cited HITRUST's frequent, threat-adaptive updates as a key element that sets it apart from other security frameworks. The HITRUST CSF framework and control selection leverages up-to-date threat intelligence, helping to ensure that HITRUST adopters continue to proactively defend against the latest cyber threats, including ransomware and phishing.

SOC 2 rarely changes, while HITRUST goes through regular updates to ensure that it matches the ever-changing threat landscape.

"HITRUST is a dynamic framework. It's a living, breathing organism, and evidence of that is in the dozens of authoritative sources," said Ali Pabrai, Chief Executive Officer at ecfirst. "Frequent updates to the CSF demonstrate that the HITRUST thought leadership is not just industry-centric, but industry-neutral. It's not just America-centric, but global. With the e1, i1 and the traditional r2 HITRUST certification options, organizations now have a credible, evidence rich framework to align their cyber and compliance strategy with their business drivers."

HITRUST is not a check-the-box exercise. But the time and effort that organizations and assessors put into the process yield reliable, consistent, and transparent results that demonstrate security maturity.

HITRUST Assessment Portfolio

Adopting the HITRUST CSF and achieving HITRUST certification can help organizations demonstrate security maturity levels, assess third-party vendors, and enhance their security posture.

The HITRUST assessment portfolio, which consists of:

- HITRUST Essentials, 1-Year (e1) Validated Assessment
- HITRUST Implemented, 1-year (i1) Validated Assessment
- HITRUST Risk-Based, 2-year (r2) Validated Assessment

The certification options allow an organization to tailor their assessment to their desired level of assurance as well as the time and effort they can devote to the process.

"The use of the proven and vetted control systems that underpin the HITRUST framework and assurance system is critical to expected security and privacy outcomes," stated Robert Booker, Chief Strategy Officer at HITRUST.

"A certification report from HITRUST provides not only assurance that the control system is measured and achieves an expected level of maturity, but also that confidence that the controls in place are those that are expected."

HITRUST Essentials, 1-year (e1) Validated Assessment

The HITRUST Essentials 1-year (e1) Validated Assessment is the ideal option for organizations looking for entry-level assurance and validation demonstrating that they have implemented vital cybersecurity controls. This option aligns with the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Essentials, the National Institute of Standards and Technology (NIST) 171's Basic Requirements, NIST IR 7621, and the Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations.

The e1 assessment may be used by low-risk businesses to demonstrate 44 foundational security controls or can be used to review third-party vendors.

Alternatively, organizations may leverage the e1 as a stepping stone to the i1 or r2. The e1 requirements can be found in the i1 and r2 assessments, giving organizations the flexibility to opt for the e1 now and take time to implement the i1 or r2 controls at a later date.

HITRUST Implemented, 1-Year (i1) Validated Assessment

The HITRUST Implemented, 1-Year (i1) Validated Assessment provides a moderate level of assurance and aligns with authoritative sources such as NIST SP 800-171 (Basic and Derived Requirements), the HIPAA Security Rule, and HICP for Medium-Sized Organizations.

The i1 can help organizations measure themselves against cybersecurity leading practices and has a broader scope than the e1. The i1 can similarly be used as a stepping stone for the r2, HITRUST's most robust and comprehensive offering. This assessment is a great option for organizations looking to demonstrate that they have implemented protections against today's top cyber threats or to ensure that their vendors have employed leading cybersecurity practices.

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

The HITRUST Risk-Based 2-year (r2) Validated Assessment provides the highest level of assurance. It aligns with dozens of authoritative sources, including HIPAA, NIST SP 800-53, the Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR).

The r2 is the gold standard for organizations that regularly process large amounts of highly sensitive data, such as financial data or protected health information (PHI). Like the e1 and the i1, the r2 can also be used for third-party risk management, ensuring that vendors hold themselves to high security standards. Achieving r2 certification can give organizations a competitive edge, demonstrating that they have implemented a robust set of security controls to protect sensitive data.

HITRUST Assessment Portfolio Features

Three cybersecurity assessment levels to meet nearly any need

e1 HITRUST Essentials, 1-Year Assessment

Focused on Foundational Cybersecurity Hygiene

For lower-risk organizations validating the most critical cybersecurity controls.

i1 HITRUST Implemented, 1-Year Assessment

Focused on Leading Security Practices

For organizations with robust information security programs ready to demonstrate implementation of controls that protect against current and emerging threats.

r2 HITRUST Risk-Based, 2-year Assessment

Focused on Expanded Capabilities

For organizations to demonstrate regulatory compliance against authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and dozens of others, or requiring expanded tailoring of controls based on identified risk factors.

Debunking Common Misconceptions About HITRUST

HITRUST's offerings are comprehensive, with many paths to certification.

"Not all HITRUST assessments are extensive, time-consuming, and expensive. The introduction of the e1 and i1 assessments brought about a range of assessments with different levels of effort," said Jeremy Huval, Chief Innovation Officer at HITRUST.

Additionally, HITRUST is more than just certifications. Any organization can access the HITRUST CSF framework free of charge.

Some organizations may even opt in to a HITRUST assessment for the purpose of identifying compliance gaps rather than achieving certification. No matter what the end goal is, HITRUST's resources can help organizations assess their security maturity levels and act accordingly.

46%

of breached organizations suffered damage to their reputations and brand value

-Forbes Institute Report

$4.35 MILLION

average cost of a data breach

-IBM Security

Another common misconception is that HITRUST is only for the healthcare sector, the industry in which it initially gained traction. While HITRUST is still focused on the healthcare sector, the framework is based on security control systems such as NIST CSF and ISO 27001, which are relevant to numerous different industries. Any organization that maintains sensitive data can benefit from HITRUST's offerings. With the addition of the e1, organizations that may not have opted for the r2 certification in the past now have the opportunity to begin their HITRUST journey on a smaller scale with similar time and resource commitments as a SOC 2 report.

"In years past, small organizations achieving HITRUST certification was not the norm given how high HITRUST set the bar," Huval noted. "The introduction of the e1 and i1 assessments and certifications changes this, as these are targeted towards organizations with lower to moderate levels of complexity and maturity. Expect more start-ups to volunteer their HITRUST e1 certification in lieu of responding to your cybersecurity questionnaire."

86%

of people are unlikely to do business with an organization that suffered a data breach involving card data

-Ponemon Institute Report

66%

of organizations were hit by ransomware last year

-The State of Ransomware, Sophos

Conclusion

Cyber threats are on the rise, and organizations must take proactive steps to mitigate risks to their data. Compliance with industry-recognized certifications, such as HITRUST, can help organizations safeguard sensitive information through adherence to robust security measures and compliance protocols. Unlike SOC 2, HITRUST offers a more prescriptive, threat-adaptive, and evidence-based journey beyond foundational security controls. HITRUST certification provides strong assurances to potential vendors about the assessed organization's security maturity level, making it a stronger and more effective certification program than SOC 2.

Produced by

TechTarget | xtelligent HEALTHCARE MEDIA

About HITRUST and ecfirst

HITRUST

HITRUST is an information protection standards organization and certifying body that enables organizations to demonstrate that they are taking the most proactive approach to cybersecurity, data protection, and risk mitigation.

Thousands of organizations across all industries safeguard their sensitive information using the HITRUST framework, assurance program, and assessment tool to meet their information protection needs.

ecfirst

Established in 1999, ecfirst delivers end-to-end compliance and cyber defense services globally. As a HITRUST Authorized External Assessor, ecfirst has successfully enabled clients to achieve and maintain their HITRUST Certification. ecfirst is among a select few organizations, to have achieved HITRUST i1 and r2 Certifications. More information at www.ecfirst.com/HITRUST.