FROM SOC 2 TO HITRUST e1:

A Comprehensive Path to Robust Cybersecurity and Trust

HITRUST®

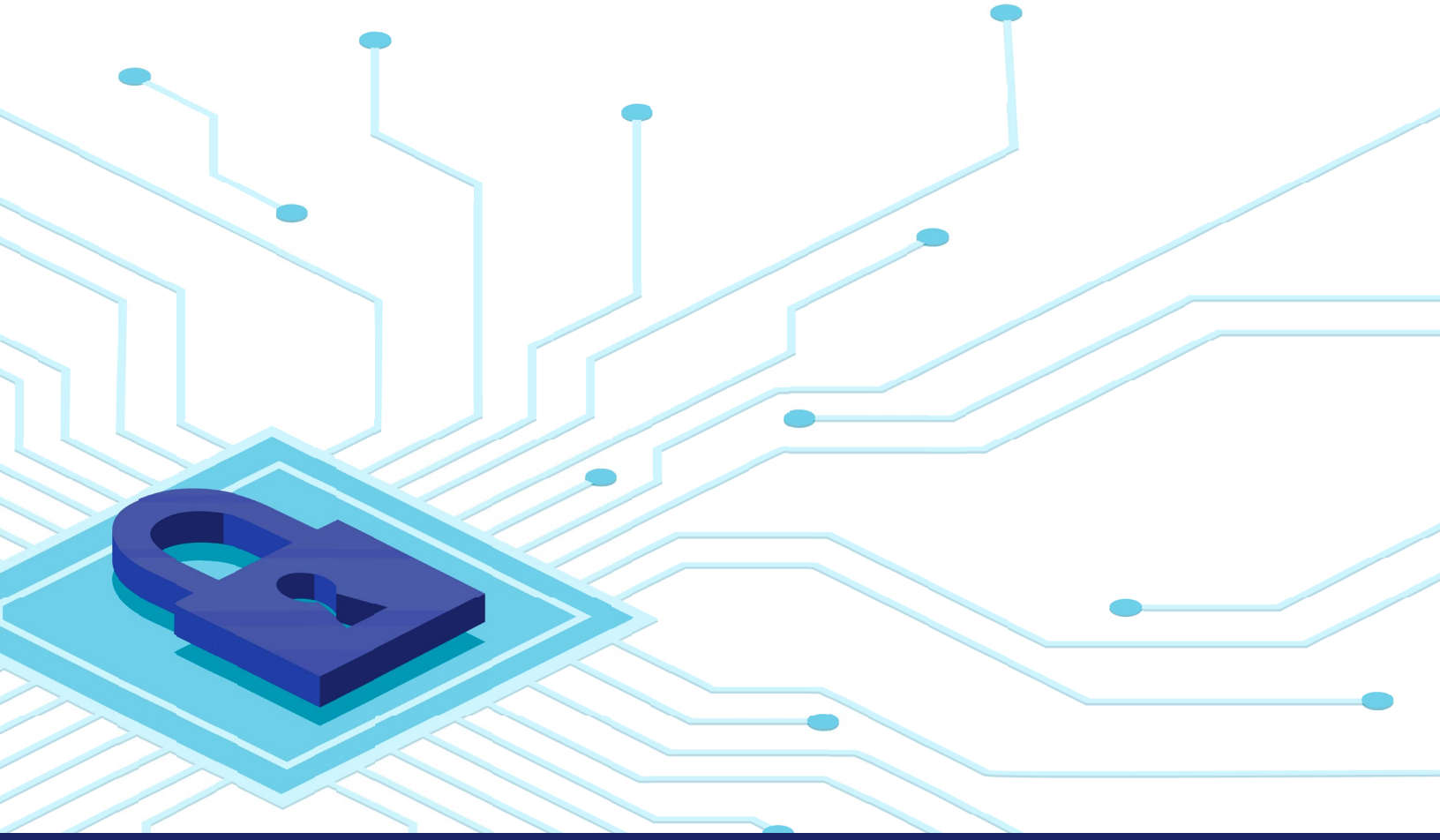
Intro

Organizations are under constant pressure to demonstrate their commitment to data security and compliance. The need for robust cybersecurity measures has never been greater, especially for businesses handling sensitive information.

HITRUST, the global leader in cybersecurity assurance, offers a prescriptive and comprehensive approach to data protection with reliable certifications that empower organizations to earn the trust of their key stakeholders. However, many organizations pursue SOC 2, either because they are required to do so or because SOC 2 provided an assurance entry point in the past.

Dive into this eBook to

- Gain insights into the differences and similarities between HITRUST e1 certification and SOC 2 attestation.
- Understand the value of a HITRUST certification, even if you have a SOC 2.
- Learn how to leverage your work toward a SOC 2 to streamline the process of attaining a HITRUST e1.



Understanding HITRUST e1 and SOC 2

What is HITRUST e1?

HITRUST offers three types of certifications — e1, i1, and r2 — to cater to varied organizational needs, sizes, and risk profiles. The HITRUST e1 focuses on the 44 most critical security controls. It is ideal for low-risk, startup, or small-sized organizations. Organizations that are not yet ready to pursue more comprehensive certifications can begin with an e1 as a starting point.

Key Characteristics of HITRUST e1

- **Certification:** HITRUST e1 offers a one-year validated certification, ensuring compliance with essential security controls.
- **Quick assessment:** The HITRUST e1 assessment can take as little as a few weeks to be completed. Most organizations obtain an e1 certification in around six to eight weeks.
- **Streamlined approach:** HITRUST e1 allows you to attain more comprehensive certifications like the i1 and r2 without losing your previous work, saving time, money, and effort.
- **Inheritance:** You can reuse and inherit controls from your own or your vendor's past assessments with the HITRUST Shared Responsibility and Inheritance Program.
- **Comprehensive framework:** HITRUST e1 is based on the HITRUST framework (HITRUST CSF), which harmonizes best practices from more than 50 authoritative sources including HIPAA, ISO, NIST, and GDPR.
- **Threat intelligence:** HITRUST leverages near real-time threat intelligence data to update its framework frequently enabling you to identify and mitigate emerging threats.

What is SOC 2?

SOC 2 is an auditing procedure developed by the American Institute of Certified Public Accountants (AICPA). It is designed for service providers to demonstrate their controls related to the Trust Services Criteria (TSC). These criteria include security, availability, processing integrity, confidentiality, and privacy.

Key Characteristics of SOC 2

- **Attestation report:** SOC 2 offers an attestation report, which is typically valid for a year.
- **Independent auditor:** An independent auditor assesses the evidence and issues the final report.
- **Customizable:** Every SOC 2 does not include all five TSC. Organizations can choose which TSC to include in their report.
- **Flexible:** SOC 2 provides general guidance on controls and allows you to describe the policies, procedures, and systems in place.

Comparing HITRUST e1 and SOC 2

Differences Between HITRUST e1 and SOC 2

There are several critical differences between the HITRUST e1 and SOC 2. Let's compare them to understand which is best for your organization.

Certification vs. Attestation	One of the most significant differences between HITRUST e1 and SOC 2 is the outcome of the assessment. HITRUST e1 results in certification, which indicates meeting rigorous standards and achieving a certain level of security maturity. A HITRUST certification offers a reliable, high level of assurance and recognition. SOC 2 results in an attestation report, reflecting the auditor's opinion on the controls without a defined minimum requirement.
Specific vs. Generic	HITRUST e1 evaluates based on specific, detailed control requirements due to its prescriptive nature. It ensures that all necessary security measures are implemented correctly. SOC 2 provides broader guidelines, giving organizations more flexibility. However, it also creates ambiguity in how they achieve compliance.
Consistent vs. Variable	All HITRUST assessments are based on the standardized, publicly available HITRUST framework, making them transparent and consistent. This means organizations from different industries and assessors undergo the same 44 controls while getting their system assessed for an e1. In contrast, SOC 2 varies significantly depending on the auditor's approach and specific controls selected by the organization.
Score vs. Judgment	HITRUST e1 and SOC 2 differ in the evaluation approach. HITRUST uses a PRISMA-based model to give quantitative scores based on the control maturity. It provides a clear and measurable indication of an organization's security posture. Results in a SOC 2 report are not scored and rely on the subjective judgment of auditors, which can lead to inconsistent evaluations.
Quality Assurance vs. Peer Review	HITRUST assessments undergo a stringent quality assurance process with six layers of checks. HITRUST reviews 100% of its assessments before issuing a certification, making it more reliable and trustworthy. SOC 2 reports are subject to minimal external review as they heavily rely on a peer review system and have only two layers of checks.

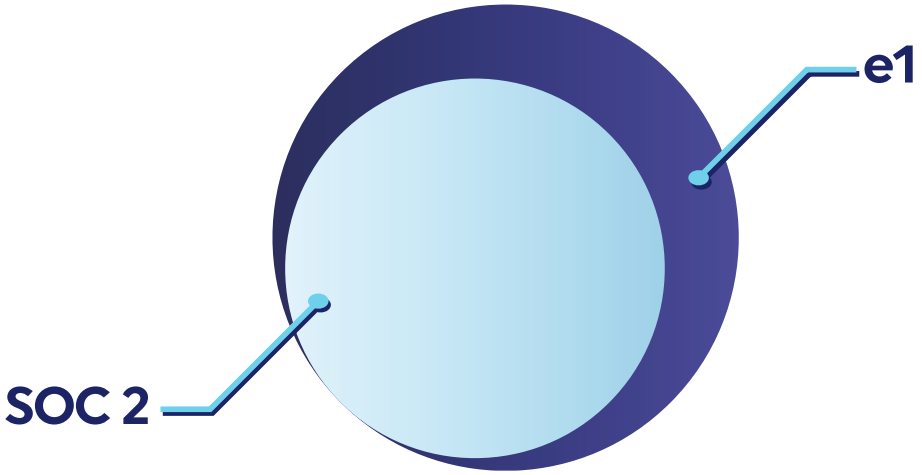
Overlapping Controls Between HITRUST e1 and SOC 2

Despite their differences, HITRUST e1 and SOC 2 are both cybersecurity assessments that evaluate controls and allow you to demonstrate cyber maturity. They have a significant overlap in controls, allowing organizations to leverage the work done for one when pursuing the other. Organizations can streamline their compliance efforts, save time, and easily get a HITRUST e1 when they already have a SOC 2 or are required to get one.

Number of Overlapping Controls

Approximately 36 of the 44 HITRUST e1 requirements map to one or more SOC 2 controls (based on all controls in all five TSC). Excluding the privacy criterion, these requirements map to all or part of 75 of the 85 SOC 2 controls, or 88%.

This means 80%–90% of the work in an e1 assessment may be utilized when performing a SOC 2, especially when privacy is excluded. The remaining level of effort is dependent on the additional controls that an organization maintains in support of the SOC 2 TSC. As SOC 2 broadly defines the expected controls and HITRUST granularly specifies its requirements, organizations must ensure they align their control environment with the e1 and then map to SOC 2 when pursuing both.



Example of Overlapping Controls

Consider controls related to data backups as an example. In SOC 2, a single control broadly defines general responsibilities such as authorizing, designing, developing, implementing, operating, and maintaining backup processes and recovery infrastructure. This gives generic requirements but the specifics of how these tasks should be carried out are left to the organization's discretion. If an organization has a regular data backup process in place, it may be sufficient to comply with this SOC 2 control requirement.

On the other hand, HITRUST e1 demands more precise measures. It specifically requires that data backups are created, maintained offline in an immutable format, stored at a remote location, and tested at regular intervals. It ensures that they cannot be altered and deleted. Organizations must complete all these steps to meet the three corresponding e1 control requirements.

This means a SOC 2 control might partially align with HITRUST e1's requirements but additional steps are necessary to meet HITRUST's higher standard. HITRUST e1 adds depth to the security measures, ensuring that critical aspects are comprehensively addressed, and data is well-protected.

Why to Pursue a HITRUST Certification

After learning about HITRUST e1 and SOC 2, the next step is to understand why pursuing a HITRUST certification could be the right move for your organization whether you already have a SOC 2, are planning to pursue one, or are starting from scratch.

HITRUST e1 offers unique advantages, addresses gaps left by SOC 2, and provides additional value. If you begin your assurance journey with a HITRUST e1, you can establish a solid foundation for your organization's security posture and set the stage for future growth.

Benefits of a HITRUST Certification

- **Comprehensive framework:** The HITRUST framework outlines robust security controls to ensure all critical steps are implemented effectively.
- **Increased trust and assurance:** Achieving HITRUST certification demonstrates a high level of commitment to security and empowers you to earn the trust of customers, partners, and other key stakeholders.
- **Enhanced security:** HITRUST's prescriptive nature ensures that your organization is better prepared to protect data and has an overall enhanced security posture.
- **Proven effectiveness:** HITRUST is the only reliable assurance proven to reduce risk. Only 0.6% of organizations with HITRUST certifications reported breaches in 2022 and 2023 as per the HITRUST 2024 Trust Report.

Challenges Addressed by HITRUST

- **Addressing gaps left by SOC 2:** HITRUST e1 fills in the gaps that SOC 2's broader controls may leave with its detailed requirements, offering more comprehensive security assurance.
- **Meeting regulatory requirements efficiently:** HITRUST's alignment with multiple authoritative sources, including HIPAA, PHIPA, and GDPR, ensures you can meet different regulatory requirements with a single assessment.
- **Managing risks:** HITRUST uses threat intelligence data to identify emerging threats and keep its framework updated. The cyber threat-adaptive HITRUST framework keeps your organization's controls aligned with the latest threat landscape, providing superior risk management.

Integrating HITRUST e1 with SOC 2

Many organizations pursue SOC 2 because it is often required by their clients or partners. However, SOC 2 alone may not be sufficient to address all security and compliance needs. If you already have a SOC 2 or are required to get one, you can leverage that work to pursue a HITRUST e1 certification efficiently.

Approaches for adding HITRUST e1 to SOC 2

Align e1 Assessment with SOC 2 Fieldwork

Pursuing a HITRUST e1 and SOC 2 concurrently enables a streamlined process and reduces duplication. This approach involves aligning the timing of SOC 2 fieldwork with the 90-day HITRUST e1 fieldwork period. It saves time and resources as controls are tested within a single audit cycle.

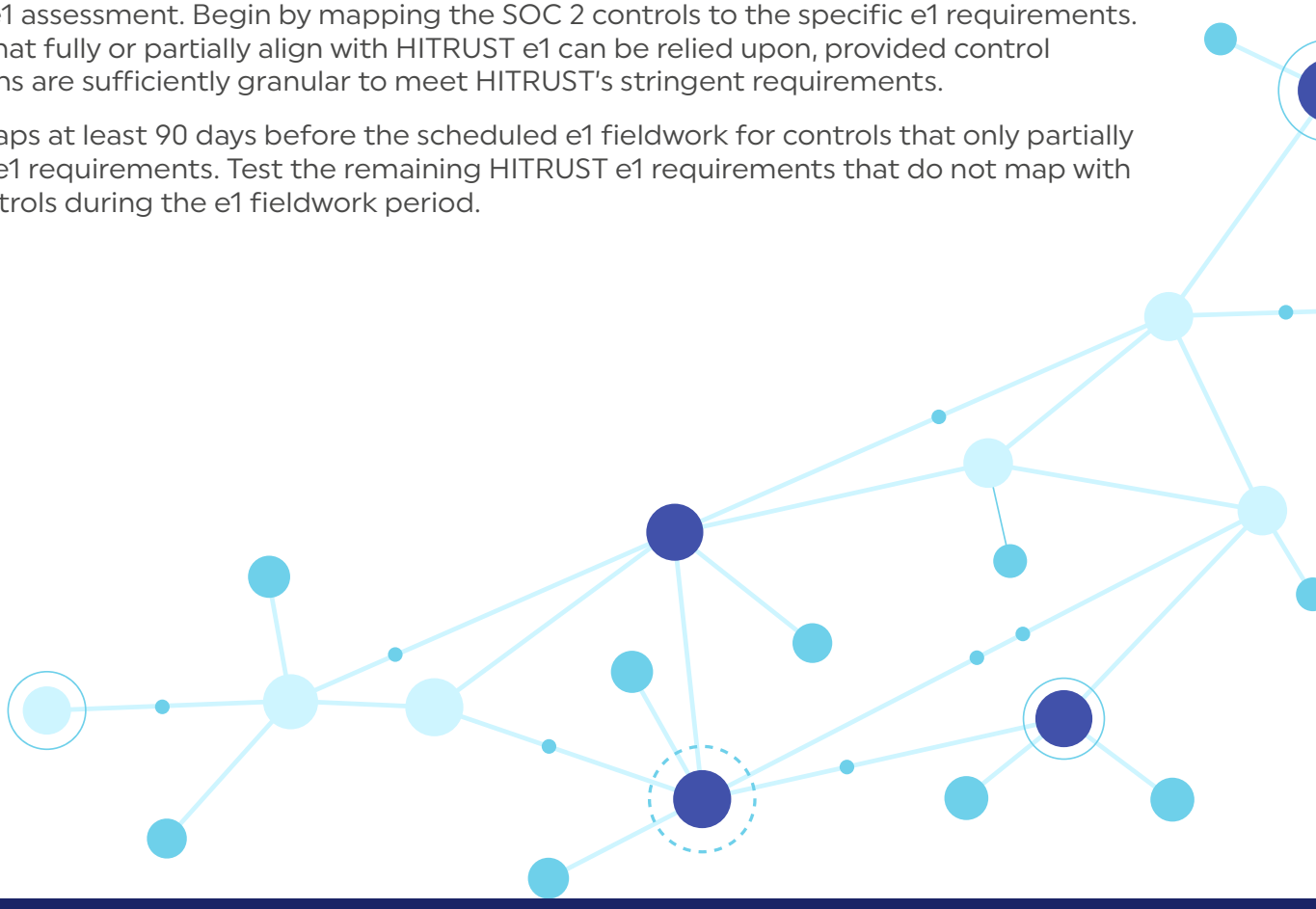
If you have identified SOC 2 controls, begin the pre-assessment by checking the corresponding HITRUST e1 requirements. Otherwise, begin by identifying controls supporting e1 requirements as they are more granular. Map e1 controls to SOC 2 and identify any additional controls. If controls partially meet HITRUST e1 requirements, conduct a review to determine the gaps that need remediation at least 90 days prior to e1 fieldwork.

Work with your External Assessor to identify efficiencies and further optimize the fieldwork periods.

Use Existing SOC 2 Report for an e1 Assessment

If you already have a SOC 2 report, you can leverage the work and use it as a foundation for the HITRUST e1 assessment. Begin by mapping the SOC 2 controls to the specific e1 requirements. Controls that fully or partially align with HITRUST e1 can be relied upon, provided control descriptions are sufficiently granular to meet HITRUST's stringent requirements.

Address gaps at least 90 days before the scheduled e1 fieldwork for controls that only partially meet the e1 requirements. Test the remaining HITRUST e1 requirements that do not map with SOC 2 controls during the e1 fieldwork period.



Benefits of HITRUST e1 alongside, after, or instead of SOC 2

- **Comprehensive assurance:** Combining HITRUST e1 with SOC 2 ensures that all critical security and privacy controls are in place, offering comprehensive protection.
- **Market differentiation:** Achieving HITRUST e1 certifications can significantly enhance your organization's credibility and give you a competitive advantage.
- **Ensuring compliance:** Getting e1 and SOC 2 enables you to meet the requirements of your clients and partners. HITRUST certifications demonstrate your organization's commitment to adhering to the highest standards of security, ensuring you are compliant with a wide range of standards and regulations.
- **Efficiency and cost-effectiveness:** Leveraging the overlap between HITRUST e1 and SOC 2 allows for a more efficient process, saving time and resources while ensuring enhanced security coverage.

Key Takeaway

As you navigate the complex landscape of cybersecurity and compliance, the decision to pursue HITRUST certification — independently or in conjunction with SOC 2 — can offer significant benefits. HITRUST e1 provides a level of assurance and protection that goes beyond SOC 2, filling in gaps and offering a more prescriptive and standardized approach to security.

If you already have a SOC 2 report, adding HITRUST e1 certification is the logical next step to enhance your overall security posture without a significant increase in effort. HITRUST e1 offers a valuable solution whether you are looking to differentiate your organization in the marketplace, meet regulatory requirements more efficiently, or ensure that your data protection measures are comprehensive and up to date.

Act Now

Don't wait to enhance your organization's security and compliance efforts. Contact the HITRUST team today to learn more about how to integrate HITRUST e1 with your SOC 2 efforts or to start your HITRUST certification journey. Secure your data, build trust, and stand out in a competitive marketplace with HITRUST.