



HITRUST vs SOC 2:

Why HITRUST is the Gold Standard for Benefits Data

When you entrust software with your employee's sensitive data, including healthcare data associated with their benefits, you need confidence the software has robust security measures in place. Why is HITRUST a better measure of compliance for employee benefits data compared to the widely used SOC 2 framework?

Threat Data vs Internal Policies

SOC 2 allows organizations to design their own controls to comply with the key trust service principles. HITRUST designates specific controls based on industry-recognized frameworks such as ISO 27001, NIST, & HIPAA. This structured approach provides assurance that a company that is HITRUST r2 certified has achieved a specific level of security consistent amongst other companies with the same designation.

Demonstrated Maturity

Earning a HITRUST certification signifies a mature security program. HITRUST requires a very rigorous assessment process, including a deep examination of an organization's policies, procedures, and implemented security controls to ensure they are proactively addressing the current threat landscape.

Reduced Risk

Choosing a HITRUST-certified vendor reduces your own security risk by ensuring robust controls are in place to protect sensitive data. This minimizes the likelihood of breaches or unauthorized access to your information. According to the [2024 Trust Report](#),* less than 1% of organizations with a HITRUST certification reported security breaches to HITRUST over 2022 and 2023.

Specificity for Healthcare

HITRUST goes beyond SOC 2's broad scope by explicitly addressing the security and privacy requirements of HIPAA and other healthcare regulations. This ensures controls are directly aligned with the most critical regulations in the employee benefits industry.

Number of Controls

HITRUST Assessments are built on the HITRUST CSF, a unified framework that combines nearly [2,000 security controls](#)** from numerous industry standards. For security-focused SOC 2 Type 2 audits, an average of [80 controls](#)*** are examined for their design and operational effectiveness.

Stronger Regulatory Alignment

A HITRUST certification allows you to incorporate specific requirements and regulations into the certification according to your industry. Within the employee benefits industry, you can include HIPAA and state-specific privacy requirements and regulations. HITRUST has the ability to map to various industry-recognized frameworks.

*<https://23257256.fs1.hubspotusercontent-na1.net/hubfs/23257256/TrustReport.pdf>

**<https://23257256.fs1.hubspotusercontent-na1.net/hubfs/23257256/Download%20Center%20%2B%20Partner%20Content/Why-the-HITRUST-Certification-is-So-Broadly-Accepted.pdf>

***<https://secureframe.com/hub/soc-2/controls>