Why It's Time to Rethink SOC 2 in Third-Party Risk Management

SOC 2 reports are no longer enough to ensure security. In a world of escalating cyber risk and increasing ransomware attacks, third-party risk programs need an assurance mechanism that actually works.

- ✓ See why SOC 2 has become a race to the bottom.
- ✓ Learn what it really takes to trust a vendor's security posture.
- ✓ Discover why leading organizations are replacing SOC 2 with HITRUST certification.

HITRUST®

The SOC 2 Dilemma in TPRM

SOC 2 used to be a signal of strong security. Now, it's nothing more than the starting line.

SOC 2

- Relies on criteria chosen by the vendor, who may lack the expertise to identify the most important threat-based controls
- Lacks alignment with most regulatory frameworks
- Doesn't guarantee standardized review or scoring process
- Often omits critical security areas
- Lacks prescriptive control requirements
- Makes it difficult to interpret what was included and compare reports

SOC 2 is the most common report accepted by security, procurement, and risk teams evaluating vendors. But its value has eroded. In many cases, SOC 2 tells you little about the maturity, rigor, or risk posture of a third party.

Why? Because today's threat landscape demands more than generic controls and auditor opinions. Organizations need assurance that's built on standardized, repeatable, and threat-adaptive evaluations. The risks of relying solely on SOC 2 are growing, and so is the cost of a bad third-party decision.

How SOC 2 Has Been Trivialized — and Why That's a Problem

SOC 2 isn't just weakened; it's been industrialized. The rise of low-cost, automated SOC 2 toolkits has created a "compliance mill" culture, where organizations are incentivized to do the minimum to get the report and move on.

The result? A flood of nearly indistinguishable SOC 2s, many of which offer limited actual assurance.

"SOC 2 has become a commodity product. The focus has shifted from doing it right to doing it quickly."

– Anecdotes.ai

Common Issues with SOC 2

- **Vendor-defined scope means some controls are simply skipped.**
  - Organizations can tailor the scope so narrowly that critical security areas, like incident response or data encryption, may not be assessed at all.
- **Auditors vary in rigor and methodology.**
  - Without a standardized testing process, the quality and depth of audits can differ dramatically, making reports unreliable for risk comparison.
- **No maturity scoring or visibility into remediation.**
  - SOC 2 doesn't indicate how well controls are implemented or whether gaps have been addressed.

And above all, many organizations accept these reports without review, perpetuating a cycle of unchecked risk.

The TPRM Wake-Up Call

Most vendor risk programs were built around a simple idea: collect SOC 2 reports, review them annually, and assume reasonable security. But that idea hasn't kept up with the threat landscape or regulatory expectations.

Today's third-party ecosystems are larger, more complex, and more vulnerable than ever. You need more than a one-size-fits-all audit. You need assurance that can scale with your vendor ecosystem.

So, what should you require from your vendors instead? HITRUST certification.

Assurance That Evolves with Risk

HITRUST certification delivers what SOC 2 cannot. Organizations that want real security proof are turning to HITRUST.

HITRUST offers effective TPRM approach with reliable assurance, relevant controls, and proven results.

- **HITRUST leverages the latest threat intelligence data to proactively monitor and protect against emerging cyber risks.**
  - The HITRUST framework is cyber threat adaptive. It is frequently updated to keep up with the evolving threat landscape.
- **The HITRUST framework is uniquely designed to align with more than 60 security, privacy, and regulatory standards.**
  - HITRUST ensures comprehensive coverage across diverse compliance requirements with its prescriptive controls to help organizations address security challenges.
- **HITRUST is the only assurance mechanism proven to reduce risk.**
  - With 99.41% of HITRUST-certified environments remaining breach-free in 2024, HITRUST actually works to strengthen cybersecurity defenses and mitigate risks.

- **HITRUST offers scalable assessment options designed to meet the specific needs of vendors.**
  - With flexibility to adapt to varying sizes and risk profiles, HITRUST provides organizations with a tailored approach to risk management.
- **HITRUST streamlines vendor management and reduces manual effort.**
  - With HITRUST TPRM Services and integration with platforms like ServiceNow, HITRUST enables managing a large volume of vendors by automating workflows and centralizing reporting.
- **HITRUST encourages continuous monitoring and remediation of gaps.**
  - HITRUST supports risk tracking and provides actionable remediation strategies, enabling vendors to proactively manage their security posture and stay resilient in an ever-changing threat landscape.

What Security Leaders Can Do Right Now

Whether you're overhauling your vendor risk program or looking to tighten standards, here's what to do next.

Reevaluate SOC 2 as a default requirement.

Ask: Does this report offer enough clarity, consistency, and rigor?

Educate stakeholders.

Update your vendors and procurement, legal, and security teams on why SOC 2 does not ensure robust security.

Accept, recommend, or require HITRUST certification.

Encourage your vendors to get HITRUST certification for improved risk management and enhanced protection.

Tier your vendors by risk.

Use the HITRUST e1 certification for lower-risk vendors or as a first step, i1 certification for medium-risk vendors, and r2 certification for high-risk vendors.

Lead the shift.

Help your industry move beyond checkbox compliance and toward true, proven assurance.

The HITRUST Advantage

HITRUST is the gold standard for organizations that need to streamline vendor risk management, reduce risk, and build trust with customers and partners. By leveraging HITRUST's standardized and comprehensive assurance processes, organizations make TPRM efficient and effective. Requiring a HITRUST certification reduces third-party risk, enhances trust in your vendor's data protection programs, and ensures that your organization stays resilient. It gives you the confidence you need to scale your business.

Ready to strengthen your vendor risk program?

Visit hitrustalliance.net/third-party-risk-management to learn how HITRUST can support your TPRM strategy.