HITRUST

Redefining Third-Party Risk Management **with the HITRUST Validated Assurance**

EXECUTIVE SUMMARY

The digital enterprise now operates in an ecosystem of thousands of third parties — each an extension of its own risk surface. Yet most organizations still rely on outdated, manual approaches to third-party risk management (TPRM). Static questionnaires and inconsistent standards have turned vendor assurance into a slow, resource-draining exercise that fails to keep pace with modern business or regulatory expectations.

As the volume and complexity of vendor relationships surge, this reactive model is no longer sustainable. Security, compliance, and procurement teams face mounting pressure to move faster while maintaining defensible oversight, but the current process creates friction instead of confidence.

How Validated Assurance Transforms TPRM

HITRUST redefines TPRM by enabling organizations to replace guesswork with validation, fragmentation with standardization, and effort with automation, delivering a proven, defensible approach to vendor assurance. By standardizing assurance across vendors, HITRUST enables organizations to manage risk with precision, efficiency, and trust.

The result is a new foundation for digital confidence,
one where third-party assurance is no longer a bottleneck, but a business accelerator.

With HITRUST validated assurance, organizations achieve

- **3–5× greater vendor assessment throughput** through standardized assurance.
- **Up to 50% lower operational costs** by eliminating redundant due diligence activities.
- **Stronger security outcomes**, with HITRUST-certified environments remaining 99.41% breach-free (HITRUST Trust Report 2025).

Validated assurance doesn't just modernize TPRM. It transforms it. It replaces uncertainty with proof, manual effort with automation, and fragmented processes with a unified approach of trust.

THE GROWING THIRD-PARTY RISK CRISIS

A Perfect Storm of Complexity and Exposure

The modern enterprise runs on a vast and interconnected vendor ecosystem. The average Global 2000 enterprise depends on more than 8,000 vendors delivering nearly 18,000 IT products and services (SecurityScorecard and Cyentia 2024).

What once consisted of a few strategic partners has multiplied into thousands of third-party relationships, each one expanding the organization's attack surface. **99% of Global 2000 organizations** are connected to vendors that have experienced recent breaches (SecurityScorecard and Cyentia 2024).

The scale is overwhelming, and so is the cost. The average third-party breach **costs $4.91 million** (IBM 2025). As digital supply chains expand, the potential for risk exposure grows exponentially. Every new integration, service provider, or SaaS connection introduces another possible point of failure.

Operational Breakdown

Traditional TPRM methods simply cannot keep up. Teams are buried in repetitive assessments, siloed documentation, and ever-changing regulatory demands. Instead of building trust, many programs now create fatigue.

Common pain points include

Unsustainable approaches: Assessment workloads continue to outpace available budgets and personnel.

Long turnaround times: Reviews drag on for weeks or months, stalling procurement and slowing innovation.

Overwhelmed vendors: Suppliers face duplicate questionnaires from every client, creating frustration and compliance burnout.

Limited remediation: Even when issues are found, they're rarely tracked to closure, leaving lingering vulnerabilities.

Blind spots: Organizations lack a single, accurate view of vendor risk across business units.

Outsized costs: The manual effort required to manage thousands of vendors consumes both financial and human resources.

For many enterprises, TPRM has become a necessary evil — a compliance checkbox rather than a meaningful line of defense.

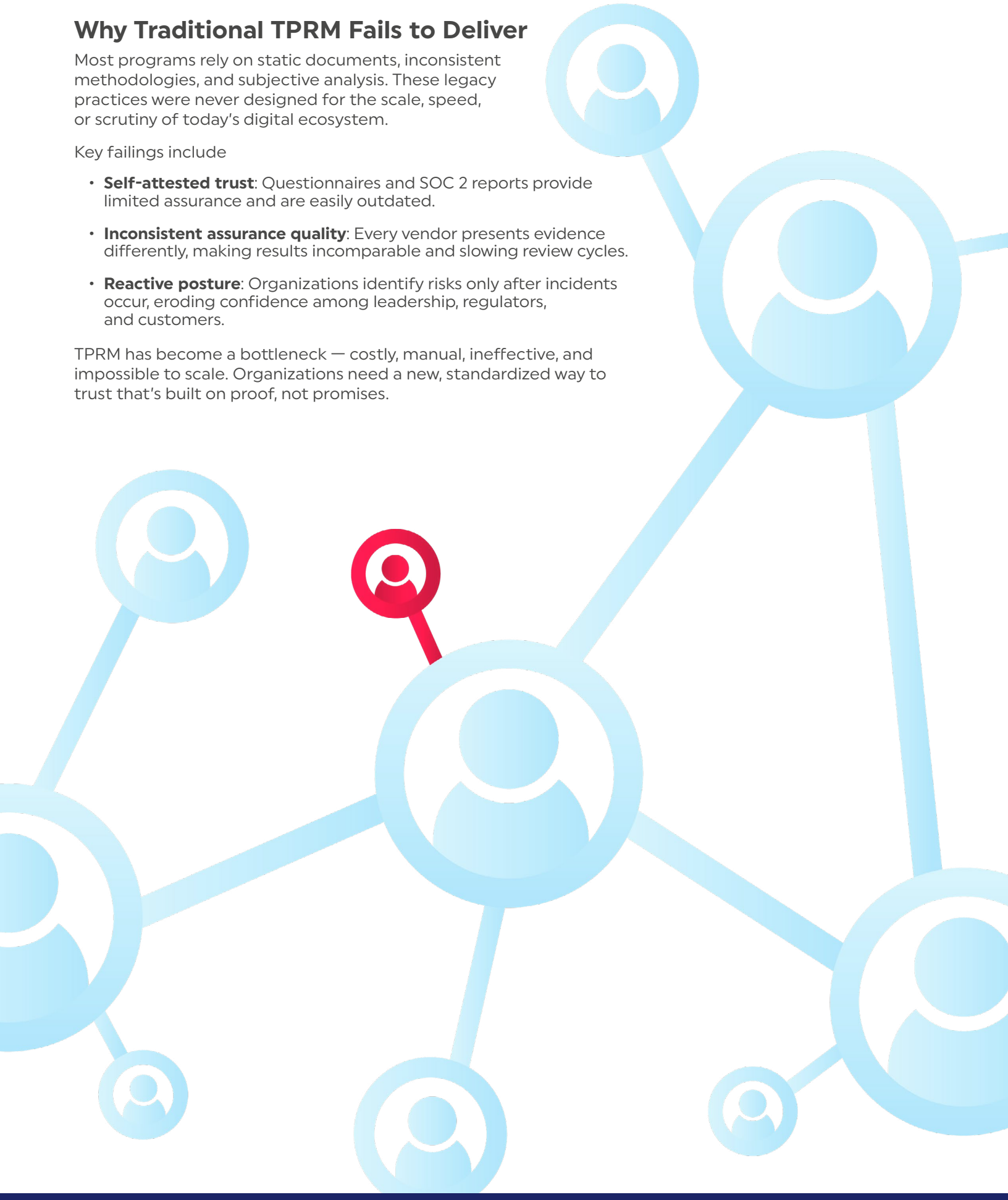
Why Traditional TPRM Fails to Deliver

Most programs rely on static documents, inconsistent methodologies, and subjective analysis. These legacy practices were never designed for the scale, speed, or scrutiny of today's digital ecosystem.

Key failings include

- **Self-attested trust**: Questionnaires and SOC 2 reports provide limited assurance and are easily outdated.
- **Inconsistent assurance quality**: Every vendor presents evidence differently, making results incomparable and slowing review cycles.
- **Reactive posture**: Organizations identify risks only after incidents occur, eroding confidence among leadership, regulators, and customers.

TPRM has become a bottleneck — costly, manual, ineffective, and impossible to scale. Organizations need a new, standardized way to trust that's built on proof, not promises.



THE SHIFT TO VALIDATED ASSURANCE

The growing scale and complexity of third-party ecosystems have made one truth undeniable: organizations can no longer rely on unverified trust. In a world where a single vendor compromise can trigger cascading losses across entire industries, confidence must be earned and proven.

That's where validated assurance comes in. HITRUST pioneered this model to give organizations confidence backed by proof. By blending verification, standardization, and risk reduction, HITRUST transforms third-party oversight into a measurable, repeatable process that strengthens both compliance and performance.

Validated Assurance: A Proven Foundation for Trust

Validated assurance replaces unverified claims and self-reported questionnaires with independent, benchmarked, and quality-controlled proof of an organization's security and privacy posture. Instead of relying on promises, enterprises gain defensible evidence of a third party's controls, verified by qualified assessors and backed by a consistent standard.

Validated assurance addresses the core weaknesses that have plagued traditional TPRM programs for years. It enables organizations to reduce risk, gain confidence, standardize evaluation, and scale growth.

The message is clear:
when trust is validated, resilience and efficiency follow.

HOW HITRUST MAKES VALIDATED ASSURANCE OPERATIONAL

While the concept of validated assurance is powerful, HITRUST makes it practical and scalable and translates it into repeatable, defensible outcomes.

Core Differentiators

Integrated Framework: HITRUST harmonizes over 60 global standards and regulations, ensuring comprehensive coverage across privacy, security, and compliance.

Tiered Assurance (e1, i1, r2): Flexible assessment levels align assurance depth to vendor criticality, optimizing rigor and efficiency.

Centralized Quality Assurance: Every assessment is independently verified through HITRUST's centralized QA process, ensuring uniform trustworthiness.

Threat-Adaptive Updates: The HITRUST Framework evolves continually, incorporating emerging threats and regulatory requirements to stay ahead of risk.

Automation and Interoperability: Integration with GRC platforms like ServiceNow through the HITRUST TPRM Services (formerly known as HITRUST Assessment XChange) enables automated workflows, seamless evidence reuse, and real-time visibility across vendor portfolios.

Standardized Control Set: Standardizing allows organizations to quickly develop efficiencies because they know exactly which controls were tested.

The Outcome

An end-to-end validated assurance ecosystem that reduces risk, accelerates trust, and delivers defensible third-party oversight at scale.

THE SIX-STEP PROCESS FOR SMARTER VENDOR QUALIFICATION

Even with stronger frameworks and better technology, many organizations still struggle to translate risk data into clear, defensible vendor decisions. HITRUST addresses this challenge with a structured, end-to-end process that ensures every vendor is evaluated, qualified, and monitored with precision and consistency.

This six-step methodology transforms third-party oversight from an administrative burden into a measurable, repeatable business process that scales.

STEP 1	**Third-Party Pre-Qualification** Engage stakeholders, review data access and processing, and assess the vendor's potential impact. This early triage step prevents wasted effort on vendors that don't meet basic security or compliance expectations. The HITRUST TPRM Services helps to streamline onboarding and manage a large volume of vendors with reduced manual effort.
STEP 2	**Risk Triage** Classify vendors by inherent risk and determine the level of assurance required. This step ensures that effort aligns with exposure, assigning HITRUST e1, i1, or r2 assessments as appropriate. The tiered HITRUST assessments help to evaluate vendors appropriately based on their size, risk profile, and business criticality.
STEP 3	**Risk Assessment** Ask your vendors to undergo a HITRUST assessment. Obtain and evaluate HITRUST Validated Assessments against defined standards. These assessments provide verifiable, benchmarked results.
STEP 4	**Risk Mitigation** Identify control gaps and review corrective action plans (CAPs) as the priority produces review efficiencies not otherwise gained through traditional due diligence. The average HITRUST r2 has 470 hours of due diligence performed before it is ever submitted for certification.
STEP 5	**Risk Evaluation** Check the vendor's remediated actions. Determine residual risk and align it with the organization's risk appetite and tolerance. This ensures defensible, transparent decision-making.
STEP 6	**Third-Party Qualification** Formally accept or reject the vendor based on total assessed risk and assurance depth. You can confidently do business with a vendor if they successfully get a HITRUST certification.

Why It Matters

This process eliminates subjectivity, reduces duplication, and ensures consistent, defensible outcomes. With HITRUST, organizations gain efficiency, visibility, and confidence in every decision backed by proof.

QUANTIFYING THE IMPACT: EFFICIENCY AND CONFIDENCE

Organizations that modernize their third-party risk management programs with HITRUST see measurable gains across four key dimensions: efficiency, cost, risk confidence, and process.

Efficiency and Scalability

Through standardized assurance and interoperable workflows, organizations can

- **Review vendors 3–5× faster** than traditional models.
- **Eliminate 8–20 hours** of low-value manual work per assessment.
- Free risk and procurement teams to focus on strategic initiatives.

Cost Control and Resource Optimization

By replacing redundant due diligence with verified certification, organizations can

- Achieve **up to 50% reduction** in TPRM operational costs.
- Reduce dependency on consulting and supplemental staff.
- Lower total cost of risk management across the vendor lifecycle.

Risk Confidence

Organizations using HITRUST experience significantly fewer incidents.

- **99.41% of HITRUST-certified environments** remained breach-free in 2024 (HITRUST Trust Report 2025).
- Centralized QA and **threat-adaptive controls** ensure consistent, defensible outcomes.

Reduced Friction

HITRUST's shared assurance model benefits both buyers and suppliers with

- Streamlined RFPs and faster procurement cycles.
- Reduced vendor pushback and audit fatigue.
- Stronger collaboration between business, security, and procurement teams.

The Outcome

Efficiency, trust, and measurable financial savings — all proven, repeatable, and sustainable.

KEY TAKEAWAY

The world of third-party risk has changed, and so must the way organizations manage it.

Traditional TPRM models built on questionnaires and static reports cannot deliver the assurance, agility, or defensibility that today's environment demands.

Validated assurance is the new foundation of digital trust — and HITRUST is its proven standard.

HITRUST redefines third-party risk management by replacing fragmented, reactive oversight with a model that is efficient, proactive, and proven. Through standardized assessments, centralized quality control, and a threat-adaptive framework, HITRUST enables organizations to assess, monitor, and trust their vendors with confidence.

With HITRUST, organizations gain

- **Speed**: Streamlined processes that reduce cycle times and accelerate procurement.
- **Confidence**: Verified, consistent evidence of control effectiveness.
- **Resilience**: Continuous assurance that evolves with emerging risks.

HITRUST empowers organizations to take control of vendor risk management by building resilience against the rising tide of third-party breaches through verified, defensible, and scalable assurance.

See how validated assurance accelerates trust and reduces third-party risk. Visit hitrustalliance.net/third-party-risk-management or contact HITRUST for a personalized briefing.