HITRUST®

TEN ISSUES CHALLENGING THIRD-PARTY RISK MANAGEMENT

WHAT THIRD-PARTY RISK LEADERS ARE TELLING US

Table of Contents

Table of Contents 2

The Top Ten Issues at a Glance 3

Executive Summary 4

Issue 1: Vendor Growth Is Outrunning TPRM Capacity 7

Issue 2: Critical Vendors Become Too Important to Fail 10

Issue 3: Lack of Assurance Comparability 12

Issue 4: Manual Work is Consuming TPRM Capacity 15

Issue 5: Hidden Vendor Risks 17

Issue 6: Incorrect or Incomplete Risk Tiering Is Directing Attention to the Wrong Places 20

Issue 7: Limited Visibility Into the Deep Supply Chain 22

Issue 8: Concentration Risk Turns Vendor Failures Into Enterprise Events 24

Issue 9: Unreliable Vendor Data Undermines Risk Decisions 26

Issue 10: Vendor Risk is Changing Faster Than Reassessment Cycles 28

Closing Perspective 30

Methodology and Inputs 32

Footnotes 33

THE TOP TEN ISSUES AT A GLANCE

A research-based view of the issues reshaping third-party risk management.

Executive Summary

Traditional Third-Party Risk Management Has Reached Its Operating Limit

Third-party Risk Management (TPRM) was built to help organizations understand and govern risk beyond their walls, but the operating model is being overtaken by the ecosystem it is meant to control. Vendor populations are expanding, critical dependencies are deepening, and the evidence used to make decisions is often incomplete, inconsistent, or already out of date.

The uncomfortable truth is that many programs are still organized to process assessments while the business needs them to manage an ecosystem and the associated risks. The result is a widening gap between the volume and speed of third-party risk and the capacity of TPRM programs to respond. Teams spend scarce expertise chasing documents, interpreting incomparable reports, and revisiting basic facts instead of identifying the exposures most capable of disrupting critical operations or compromising sensitive data.

Why This Is Needed Now

Third-party dependence has crossed from a procurement concern into a material source of enterprise exposure. Organizations are adding vendors, concentrating critical operations in a smaller number of providers, inheriting deeper supply-chain dependencies, and relying on point-in-time reviews while risk changes continuously.

The evidence shows that the operating environment is accelerating faster than the traditional review cycle:

- Nearly half of breaches now reach the enterprise through the ecosystem: the 2026 Verizon Data Breach Investigations Report found that 48% of breaches involved a third party, a 60% year-over-year increase.[1]
- The World Economic Forum reported that 54% of large organizations identify supply-chain interdependencies as the greatest barrier to achieving cyber resilience.[2]
- KPMG found that only 15% of TPRM leaders have high confidence in the data underpinning their programs, while just 18% report that TPRM is fully integrated with enterprise risk management.[3]

Research from HITRUST and CHIME[4] (see Methodology section) surveyed over 100 qualified TPRM leaders and found that:

- Nearly 55% of surveyed organizations manage more than 1,000 vendors, yet only 9.8% reported more than 20 dedicated TPRM personnel.
- About 62% said their programs would not scale if vendor counts increased by more than 30%, 48% said they cannot keep pace with assessment volume and 39% reported onboarding delays caused by backlogs.
- Every surveyed organization reported discovering at least one vendor gap or vulnerability after approval, and approximately 23% said a vendor incident had caused clinical or operational disruption.

The constraints are not on how much organizations spend. Although 81.4% of respondents reported annual TPRM program costs of at least $1 million, cost ranked last among the challenges presented. TPRM leaders placed greater emphasis that their operating model produces timely, trustworthy decisions at scale.

Together, the issues describe an interconnected operating problem: **How can TPRM programs scale without sacrificing the rigor, timeliness, and confidence required to protect critical operations and data?**

Introducing the TPRM Top 10

The operating problem facing TPRM leaders is no longer whether third-party risk matters. It is where to focus limited resources, expertise, and investment when vendor ecosystems are expanding faster than traditional review models can keep up. Answering that question requires moving beyond general concern and identifying the operational challenges most likely to determine whether TPRM can scale with the business, sustain confidence in risk decisions, and protect critical operations and data.

The TPRM Top 10 is a new perspective on the most pressing issues confronting modern third-party risk programs. These issues are the ones shaping board discussions, slowing vendor decisions, and consuming scarce expertise. Developed from HITRUST's ongoing work with TPRM leaders and practitioners responsible for complex third-party ecosystems, it reflects what programs are seeing in the field and where they believe change is most urgently needed.

This list is not presented as a universal ranking or approach for all organizations. Instead, it is intended as practical guidance for TPRM leaders to modernize their programs. Together, these issues define the work required to move from process-centered vendor review to a more scalable, evidence-driven, and enterprise-relevant model for managing third-party risk.

#	Issue	What it means
1	**Vendor Growth Is Outrunning TPRM Capacity**	Vendor populations are expanding faster than TPRM teams can add staffing and review capacity, leaving parts of the vendor portfolio under-reviewed.
2	**Critical Vendors Become Too Important to Fail**	Some vendors are so critical to business functions that organizations have little practical ability to reject or replace them, even when assessments identify material concerns.
3	**Lack of Assurance Comparability**	Inconsistent scoring and reporting methods make it difficult to compare assurance reports and results across vendors.
4	**Manual Work is Consuming TPRM Capacity**	Spreadsheets, questionnaires, and disconnected tools consume capacity that should be spent evaluating and reducing risk.
5	**Hidden Vendor Risks**	Vague scopes, inconsistent assurance methods, and limited exception reporting can obscure material control gaps until a vendor has already been approved.
6	**Incorrect or Incomplete Risk Tiering Is Directing Attention to the Wrong Places**	Incorrect or incomplete tiering makes it harder to identify which vendors pose the greatest exposure, spreading scarce resources too thin.
7	**Limited Visibility Into the Deep Supply Chain**	Organizations often lack a clear view of the subcontractors and other downstream parties supporting their most critical vendors.
8	**Concentration Risk Turns Vendor Failures Into Enterprise Events**	Heavy dependence on a small number of providers can turn one vendor incident into a broader enterprise disruption.
9	**Unreliable Vendor Data Undermines Risk Decisions**	Incomplete or unreliable information weakens risk decisions and delays action.
10	**Vendor Risk is Changing Faster Than Reassessment Cycles**	Without timely reassessment, material changes in a vendor's security posture can go undetected between formal reviews

Emerging Themes from the Top 10

Across the ten issues, **four** areas consistently appear:

- **Focus**: Apply accurate risk tiering so the strongest requirements and most experienced judgment are directed toward the vendors that can create the greatest harm.
- **Trust**: Require independently validated assurance that makes scope, control coverage, exceptions, and shared responsibilities clear.
- **Scale**: Automate routine evidence collection, control mapping, and reassessment activity so analysts can spend more time evaluating and reducing material risk.
- **Transparency**: Extend ecosystem visibility beyond individual vendors to downstream providers, shared platforms, and concentration points.

The answer is not another questionnaire or spreadsheet. The stronger model is both risk-based and evidence-driven. It directs attention to the vendors and control areas where failure would have the most significant consequences. Instead of requiring organizations to repeatedly collect the same evidence, it relies on reusable assurance that has been independently validated. The model also supports more effective oversight by linking monitoring activities to events which can change a vendor's risk profile over time.

These 10 issues are connected symptoms of an operating model struggling to keep pace with modern third-party ecosystems. They capture the key areas where TPRM leaders report their programs are breaking down, with the objective of equipping organizations to address these challenges in order to make more timely, defensible risk decisions.

VENDOR GROWTH IS OUTRUNNING TPRM CAPACITY

Vendor populations are expanding faster than TPRM teams can add staffing and review capacity, leaving parts of the vendor portfolio under-reviewed.

Why It Matters

Third-party ecosystems now include cloud providers, software companies, data processors, managed service providers, consultants, and other external parties. Each relationship can extend cybersecurity, privacy, compliance, and resilience risk beyond the organization's direct control. Yet the teams responsible for reviewing those relationships remain comparatively small.

The result is a capacity problem with direct business consequences. When assessment demand exceeds available resources, TPRM programs must choose which vendors receive a thorough review, which receive limited scrutiny, and which wait in a growing queue. Procurement slows, onboarding becomes a bottleneck, and full-portfolio due diligence becomes increasingly difficult to sustain.

> "You're not able to actually do due diligence on your full vendor portfolio because you don't have enough people."
>
> **- TPRM Leader commenting on their capacity concerns**

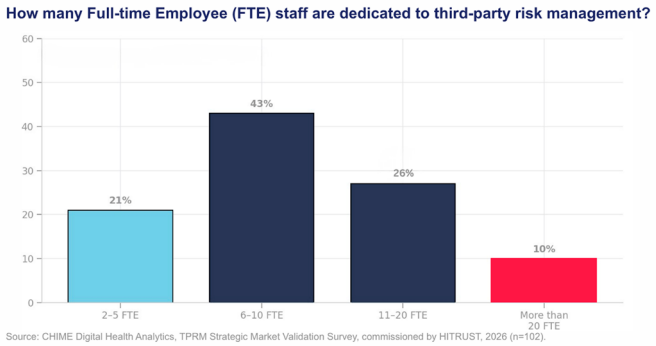
What the Evidence Shows

According to the CHIME survey:

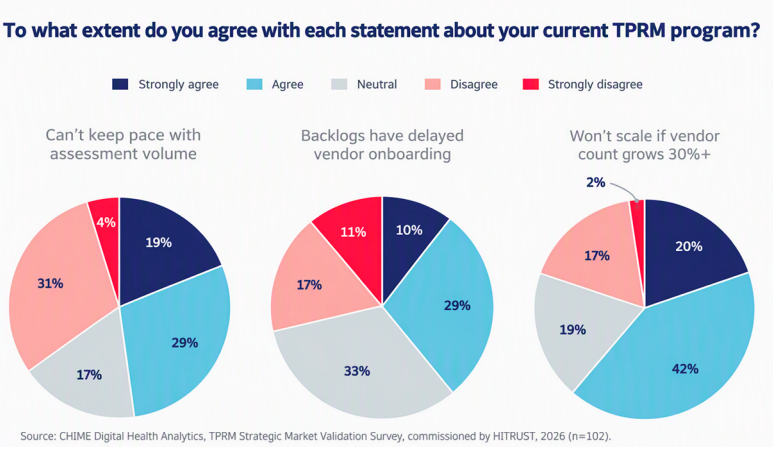
- Nearly 55% of surveyed organizations manage more than 1,000 vendors, and almost 25% manage more than 2,500.



- Only 9.8% reported more than 20 dedicated TPRM personnel.



- Almost 62% agreed that their programs would not scale if vendor counts increased by more than 30%.
- 48% of TPRM leaders agreed they can't keep pace with assessment volume, while 39% indicated they already have backlogs which have delayed vendor onboarding.



External research also reinforces these findings:

- The Venminder State of Third-Party Risk Management 2025[5] paper reports, "Despite managing more vendors, TPRM staffing has not increased proportionally. Programs with 1-2 full-time employees rose from 43% to 48%, while those with 6-10 FTEs dropped significantly (from 10% to 4%)."
- The Ncontracts State of Third-Party Risk Management 2026[6] report states, "Most TPRM programs operate with minimal staffing while managing substantial vendor portfolios. Nearly two-thirds (63%) run on just 1-2 dedicated employees, and another 13% have no dedicated staff at all. At the same time, over half (53%) manage 300+ vendors, creating ratios where individual professionals oversee 100+ vendor relationships."

What TPRM Leaders Can Do

- Apply risk-tiered assurance so the most rigorous reviews are reserved for the relationships capable of causing the greatest harm.
- Use standardized, independently validated assurance to reduce repetitive review work and reliance on one-off evidence requests.
- Automate evidence collection, control mapping, reminders, and routine reassessment activity where human judgment is not required.

While all vendors should be known and risk-tiered, the goal is not to review every vendor in exactly the same way. It is to preserve meaningful coverage as the vendor population grows, without allowing speed to replace rigor or backlogs to define the risk strategy.

CRITICAL VENDORS BECOME TOO IMPORTANT TO FAIL

Some vendors are so critical to business functions that organizations have little practical ability to reject or replace them, even when assessments identify material concerns.

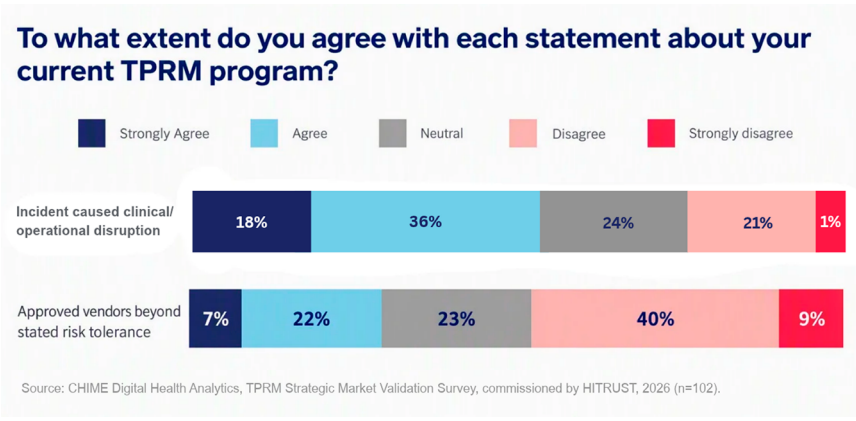
Why It Matters

Some vendors are embedded so deeply in business environments that the organization has few alternatives. Migration costs, delivery deadlines, service dependencies, and a lack of credible replacements weaken the influence of the TPRM program precisely when the potential impact is greatest.

In these cases, approval can become the expected outcome rather than the result of an open risk decision. TPRM teams may be asked to document a path forward even when the available evidence is incomplete or worse, the identified risk exceeds policy. The organization still carries the exposure, but accountability for accepting it may remain unclear.

What the Evidence Shows

- Approximately 29% of CHIME survey respondents agreed or strongly agreed that their organizations had approved vendors beyond stated risk tolerance.
- The other CHIME response by TPRM leaders demonstrates the potential impact of these approvals: About 22.6% reported that a vendor incident had caused clinical or operational disruption.



What TPRM Leaders Can Do

- Creation and executive agreement on a decision rights and accountability model, to be able to assign explicit ownership for any approval beyond stated risk tolerance.
- Document the rationale, material exposure, mitigating controls, and conditions of approval.
- Set time-bound remediation requirements and enhanced monitoring for unresolved risk.
- Test continuity arrangements and define an exit or substitution plan, even when replacement is not immediately practical.

Criticality does not reduce vendor risk. It raises the cost of failure and narrows the organization's options, making transparent governance and accountable risk acceptance more important.

LACK OF ASSURANCE COMPARABILITY

Inconsistent scoring and reporting methods make it difficult to compare assurance reports and results across vendors.

Why It Matters

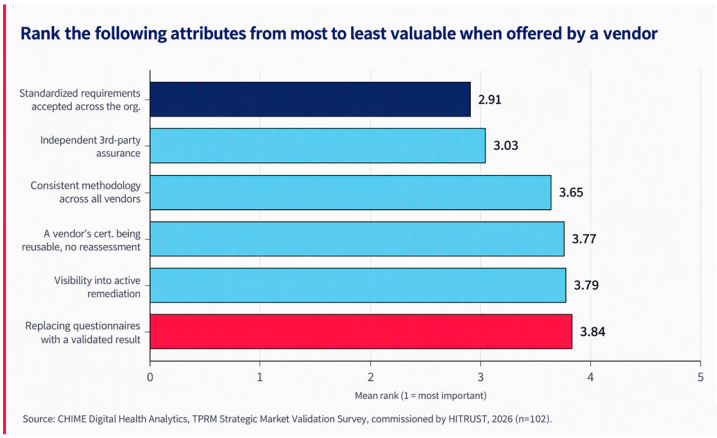
TPRM teams receive multiple forms of evidence to evaluate: Questionnaires, SOC 2 reports, HITRUST certification reports, penetration test results, vulnerability scans, and much more. Each artifact answers different questions and may use a different scope, testing method, treatment of exceptions, and reporting format. Reviewers must normalize the evidence before they can compare vendors or explain why one finding matters more than another.

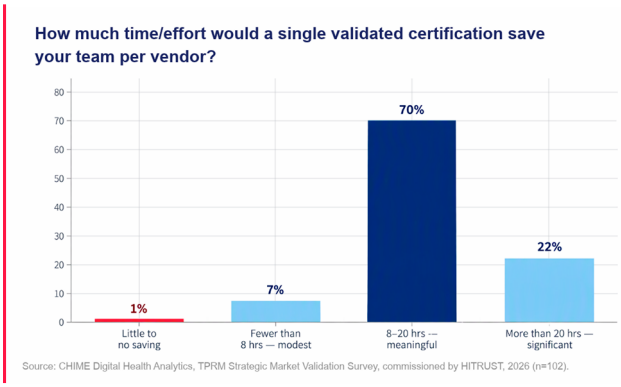
That work depends heavily on analyst experience and repeated interpretation. Two vendors can appear to provide similar assurance while covering different systems or controls. The same weakness can be described in different terms or reported at a different level of detail. Comparison becomes a manual judgment exercise rather than a repeatable program capability.

What the Evidence Shows

According to the CHIME survey:

- Standardized requirements accepted across the organization and independent third-party assurance were the two most-valued attributes in the future-state model.
- 92% of respondents estimated that relying on a single validated certification could save at least eight hours per vendor assessment. An organization assessing 100 vendors per year could save 800 hours, or 100 business days, by utilizing this strategy.





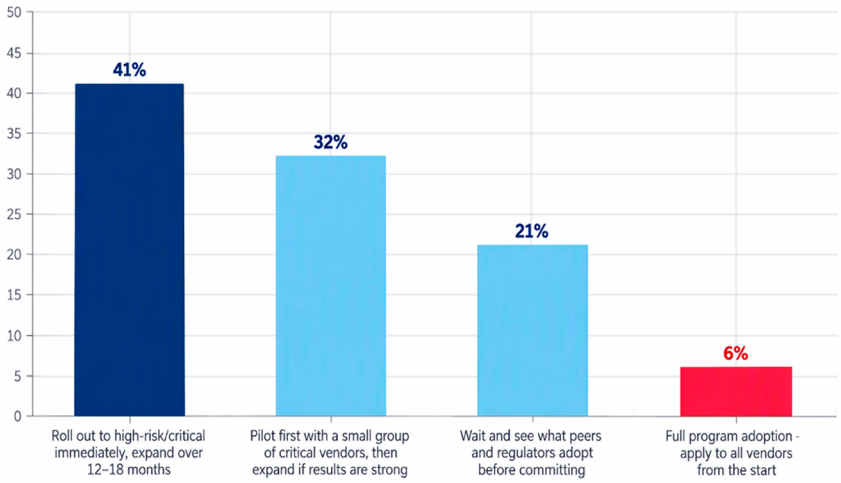
What TPRM Leaders Can Do

- Define a consistent baseline for scope, control coverage, testing, and exception reporting across assurance mechanisms.
- Use common criteria to evaluate the relevance and severity of findings, regardless of the format in which they arrive.
- Increase reliance on standardized, independently validated evidence that can be reused across vendor relationships.
- Reserve supplemental requests for material gaps in coverage instead of repeating evidence already validated.

Requiring a single standardized certification can provide tremendous benefit to TPRM programs, both in reducing risk and increasing efficiency.

Requiring a single standardized certification can provide tremendous benefit to TPRM programs, both in reducing risk and increasing efficiency. Standardized independent validation can provide a more comparable baseline across a TPRM program's vendors. When moving to adopt a standardized assurance model, the CHIME survey reported mixed results with how TPRM leaders would approach the process. Most programs (41%) would roll it out to high-risk vendors immediately and then expand to other vendors over the next year, while others (32%) would prefer to pilot first with a smaller group of those critical vendors.

If you moved to a new standardized assurance model, how would you adopt it?



Source: CHIME Digital Health Analytics, TPRM Strategic Market Validation Survey, commissioned by HITRUST, 2026 (n=102).

The goal is not to conduct the same exhaustive assessment for every vendor, but to produce enough trustworthy information to identify material exposures early and direct limited expertise toward the risks capable of causing the greatest business impact.

MANUAL WORK IS CONSUMING TPRM CAPACITY

Spreadsheets, questionnaires, and disconnected tools consume capacity that should be spent evaluating and reducing risk.

Why It Matters

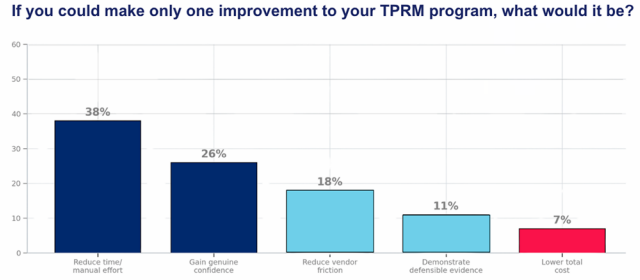
Many TPRM programs still depend on fragmented workflows. Teams track vendors in spreadsheets, distribute proprietary questionnaires, collect documents through email, and reconcile evidence manually. Each handoff adds time without necessarily improving the quality of the final decision.

HITRUST conversations with TPRM leaders reflect the issue. One TPRM leader described their process as tracking vendors in a Google Sheet, distributing questionnaires, and separately collecting security documentation. They only began the assessment once all those materials had been returned.

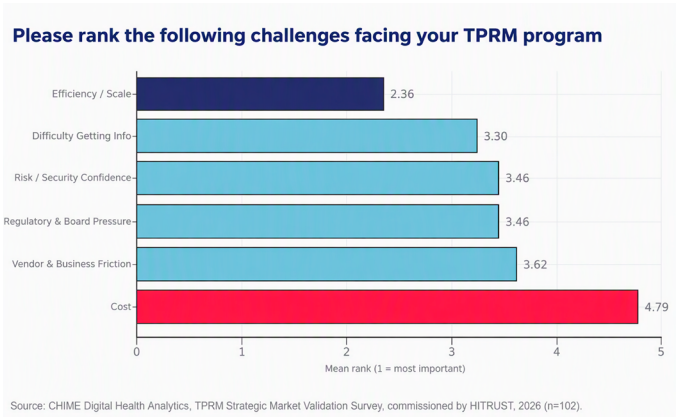
The problem is larger than the absence of a workflow platform. Digitizing the same questionnaire and document chase can preserve the underlying inefficiency. Programs need consistent assessment methods, reusable evidence, and automation that removes administrative work from trained analysts.

What the Evidence Shows

- The most selected improvement in the CHIME survey was "Reduce time and/or manual effort", chosen by 38.2% of respondents.



- "Efficiency/Scale" was identified as the highest ranked challenge facing TPRM programs.



- According to the Mitratech 2025 Third-Party Risk Management Study[7], 41% of respondents still used spreadsheets as their primary TPRM tool.

What TPRM Leaders Can Do

- Use tools to centrally manage vendor evidence, records and monitoring so reviewers do not reconstruct the vendor record for each decision.
- Automate routine evidence collection, control mapping, reminders, and reassessment triggers.
- Use AI-assisted review where it can accelerate interpretation, while keeping human judgment focused on scope, exceptions, and material risk.

Automation should change where people spend their time. The measure of progress is whether analysts have more capacity to evaluate risk and support timely decisions.

HIDDEN VENDOR RISKS

Vague scopes, inconsistent assurance methods, and limited exception reporting can obscure material control gaps until a vendor has already been approved.

Why It Matters

Vendor due diligence is intended to identify material weaknesses before the organization commits to the relationship. In practice, TPRM teams often receive evidence that is difficult to interpret or incomplete for the product or service being provided. Reports may be unclear about what was tested, which systems were included, or how deeply controls were evaluated.

HITRUST conversations with TPRM leaders identified that material risks can remain obscured even when documentation is available. TPRM leaders reported receiving assurance reports that were vague about scope, exceptions, and shared responsibilities. This forces TPRM analysts to interpret inconsistent evidence and request supplementary information before they can determine whether an identified weakness is relevant to the systems or services on which the organization depends.

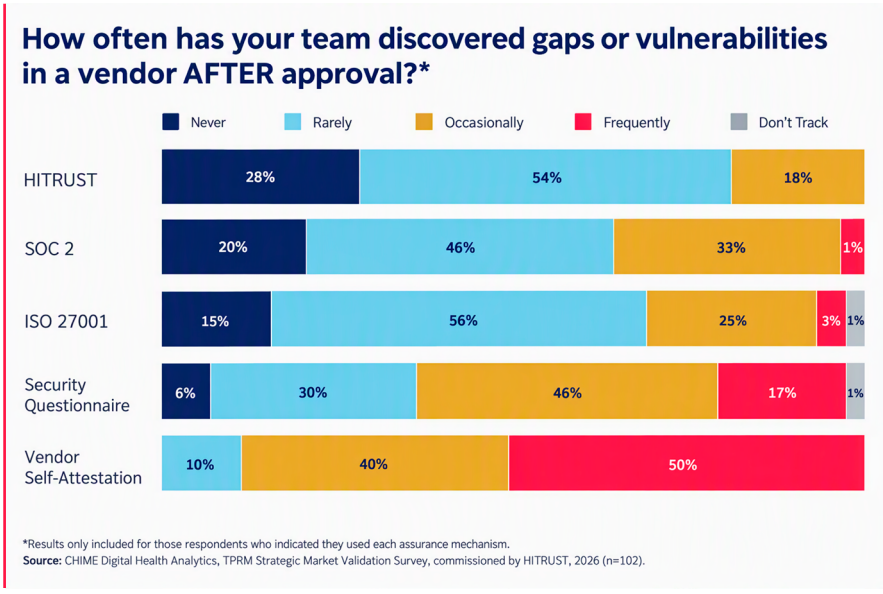
> "You don't understand fully what they actually tested versus what they didn't."
>
> **- TPRM Leader commenting on their assurance review process**

This creates a dangerous form of uncertainty. Documentation may be available, but the team still cannot determine whether the evidence covers the product or services on which the organization will rely. Additional follow-up requests may close some gaps, but they also increase review time and vendor friction.

What the Evidence Shows

In the CHIME survey:

- 100% of organizations reported that their TPRM team discovered at least one gap or vulnerability in a vendor after approval, with **18.6% of the programs frequently identifying gaps or vulnerabilities**.
- 16.7% of respondents reported that they frequently discovered vendor gaps after approval when only using security questionnaires.
- However, when organizations evaluated vendors using a third-party verified assurance mechanism (i.e. HITRUST, SOC 2, or ISO 27001) **only 2.9% of programs frequently had a vendor gap or vulnerability after approval (and none were frequent when using HITRUST)**



Additionally, the 2026 Panorays CISO Survey for Third-Party Cyber Risk Management[8] found that "while 60% of CISOs report an increase in third-party security incidents, only 15% say they have full visibility into those risks."

What TPRM Leaders Can Do

- Require evidence that clearly identifies scope, control coverage, exceptions, and shared responsibilities.
- Evaluate whether the assurance applies to the specific service, data, and operational dependency under review.
- **Use independently validated assurance for higher-risk vendors and define when supplemental evidence is still required**.
- Connect identified gaps to remediation, mitigating controls, contractual protection, or explicit risk acceptance before approval.

INCORRECT OR INCOMPLETE RISK TIERING IS DIRECTING ATTENTION TO THE WRONG PLACES

Incorrect or incomplete tiering makes it harder to identify which vendors pose the greatest exposure, spreading scarce resources too thin.

Why It Matters

Risk tiering is the mechanism that turns a large vendor inventory into a manageable set of priorities. It determines which vendors require deeper evidence, stronger contractual protections, and closer monitoring.

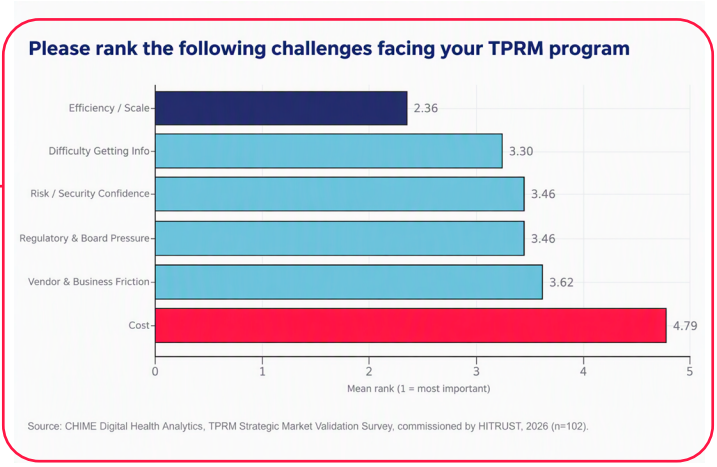
The organization's tiering model may be correct, but a polished tiering model cannot compensate for unreliable or incomplete inputs. If vendors are placed into incorrect tiers (or not placed in a tier at all), every decision that follows can also be wrong. Lower risk relationships can absorb disproportionate attention while vendors tied to critical operations or sensitive data receive too little scrutiny.

> "We probably have tens of thousands of vendors and all we've risk rated since I've been here has been like 4,000."
>
> **- TPRM Leader commenting on their risk tiering abilities**

Risk tiers depend on accurate vendor data. Organizations may be making prioritization decisions from an unreliable foundation without receiving the necessary responses and evidence from their vendors.

What the Evidence Shows

- Difficulty obtaining vendor information ranked as the second most important challenge in the CHIME survey, with risk confidence following close after.



- The KPMG 2026 Global Third-Party Risk Management[3] survey identified that only 15% of TPRM leaders had high confidence in the data that underpins their program, and only 18% were fully integrated with Enterprise Risk Management (ERM).

What TPRM Leaders Can Do

- Define tiering criteria around the business impact of vendor failure, the sensitivity of data involved, system access, operational dependency, and downstream reliance.
- Align assurance requirements with each tier instead of applying the same questionnaire or review depth to every vendor.
- Revisit a vendor's tier when its service scope, data access, dependencies, or operational role changes.
- Document and make visible exceptions and overrides so business pressure does not quietly weaken the tiering model.

A defensible TPRM program directs the strongest evidence and most experienced judgment toward the relationships that can create the most consequential loss.

> **"In our extensive experience helping design and manage TPRM programs for clients, we see companies with tens of thousands of vendors trying to screen everyone, when only a smaller fraction—perhaps 10 to 20 percent—pose higher risks that warrant deeper investigation."**
>
> - KPMG 2026 Global Third-Party Risk Management Survey

LIMITED VISIBILITY INTO THE DEEP SUPPLY CHAIN

Organizations often lack a clear view of the subcontractors and other downstream parties supporting their most critical vendors.

Why It Matters

Most TPRM programs are designed around direct contractual relationships. The service delivered by a third party, however, may depend on a deeper network of providers that store data, host applications, supply software, or support critical operations. Those fourth and deeper parties (often referred to as 4th or Nth parties) can affect the organization without appearing in its vendor inventory or participating directly in its assurance process.

The blind spot becomes more serious when assurance documentation is vague about subservice organizations, inherited controls, and shared responsibilities. A report may appear comprehensive while excluding the provider that operates an important part of the service. The TPRM team must then determine whether the dependency was assessed, carved out, or left unexamined.

> "We just have so many problems from a fourth-party perspective of getting a good understanding of who all is involved, right? And some of our third parties are like, here have this report. It'll give you all the answers you need and some of it's so vague."
>
> **- TPRM Leader commenting on their challenges with vendor assurance**

What the Evidence Shows

- According to the 2025 Panorays CISO survey[8], only 3% of organizations had full insight across their entire supply chain.
- In the World Economic Forum Global Cybersecurity Outlook 2026[9], 78% of CEOs of highly resilient organizations cited supply chain and third-party dependencies as the most significant challenge to further strengthening resilience.

What TPRM Leaders Can Do

Organizations may outsource a service, but they still retain the risk created by the supply chain behind it. Visibility must extend far enough to understand who supports critical outcomes and where assurance stops.

- Require key vendors to disclose the downstream providers supporting material services and data flows.
- Determine whether those providers and their controls are included in the assurance scope, or any supporting evidence.
- Seek separate assurance when a material dependency is excluded.
- Require notification when significant subcontractors, platforms, or service dependencies change.

CONCENTRATION RISK TURNS VENDOR FAILURES INTO ENTERPRISE EVENTS

Heavy dependence on a small number of providers can turn one vendor incident into a broader enterprise disruption.

Why It Matters

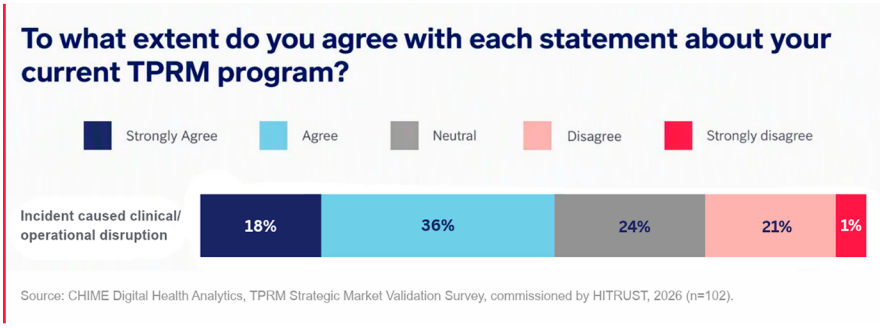
Traditional vendor reviews examine one relationship at a time. Concentration risk only becomes visible when the organization steps back and looks across the portfolio. Several vendors may rely on the same cloud platform, data processor, software, or geography. A single disruption can therefore affect multiple business processes at once, even when each direct vendor appeared manageable on its own.

The risk is especially pronounced when the underlying provider supports critical operations and few substitutes exist. The same factors that make a vendor strategically important can also make recovery slower, migration more expensive, and business pressure more intense. Relationship-level approval does not answer the portfolio-level question of how much dependency the enterprise has accumulated.

> "...a single vulnerability in a third party can quickly ripple across the entire business, grinding operations to a halt."
>
> **- KPMG 2026 Global Third-Party Risk Management Survey**

What the Evidence Shows

- According to the 2023 EY Global Third-Party Risk Management Survey[10], only 9% of organizations included concentration risk in the Risk Inventory Reporting process.
- Avoiding concentration risk requires understanding the supply chain. As noted in the Panorays 2025 CISO Survey[8], only 3% of organizations had full insight across their entire supply chain.
- The CHIME survey found that vendor incidents had already caused clinical or operational disruption for approximately 22.6% of respondents.



What TPRM Leaders Can Do

- Map critical business processes to the vendors and shared service providers that support them into a portfolio for enhanced visibility.
- Analyze concentration by provider, platform, service category, and geography across the portfolio.
- Include downstream providers when evaluating concentration and continuity exposure.
- Define contingency, substitution, and exit plans for dependencies that exceed the organization's practical tolerance.

Concentration risk is often created gradually, one reasonable vendor decision at a time. Managing it requires a portfolio view that shows where several acceptable relationships combine into one unacceptable dependency.

UNRELIABLE VENDOR DATA UNDERMINES RISK DECISIONS

Incomplete or unreliable information weakens risk decisions and delays action.

Why It Matters

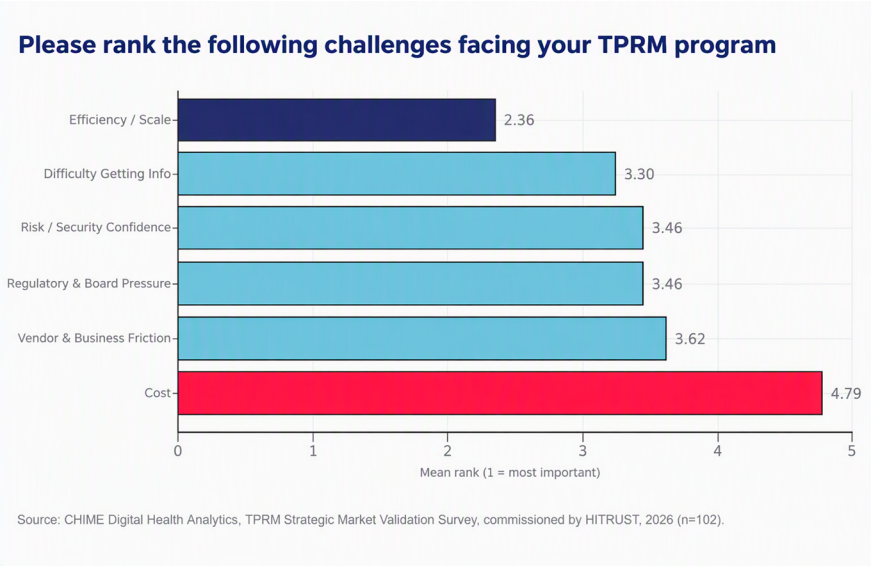
For vendors already known to the organization, the central challenge is often the quality of the information available. Assurance artifacts may omit critical details, provide vague descriptions, or fail to demonstrate the vendor's actual security posture. TPRM teams then spend additional time asking questions and requesting evidence that should have been clear at the outset.

Poor data can distort onboarding approval decisions, risk tiering, and offboarding resulting in higher risk to the organization. If a relationship is misclassified or its scope is misunderstood, the organization may apply the wrong level of due diligence throughout the vendor lifecycle.

> "I don't like wasting time with them back and forth, back and forth, back and forth"
>
> **- TPRM Leader commenting on the challenges with vendor evidence**

What the Evidence Shows

- In the CHIME survey, "Difficulty getting information" ranked as the second most important challenge.



TPRM leaders consistently describe to HITRUST their problems receiving assurance artifacts that leave critical questions unanswered regarding scope, inherited controls, fourth-party dependencies, and actual security effectiveness.

What TPRM Leaders Can Do

- Set minimum information requirements for scope, data handling, control coverage, and exceptions.
- Use standardized, independently validated evidence to improve consistency and reduce repeated follow-up.
- Treat data quality as a control over the TPRM process because weak inputs can invalidate sound review methods.

TPRM programs do not need more documents for their own sake. They need complete, trustworthy, and decision-ready information that can support consistent risk judgments.

VENDOR RISK IS CHANGING FASTER THAN REASSESSMENT CYCLES

Without timely reassessment, material changes in a vendor's security posture can go undetected between formal reviews.

Why It Matters

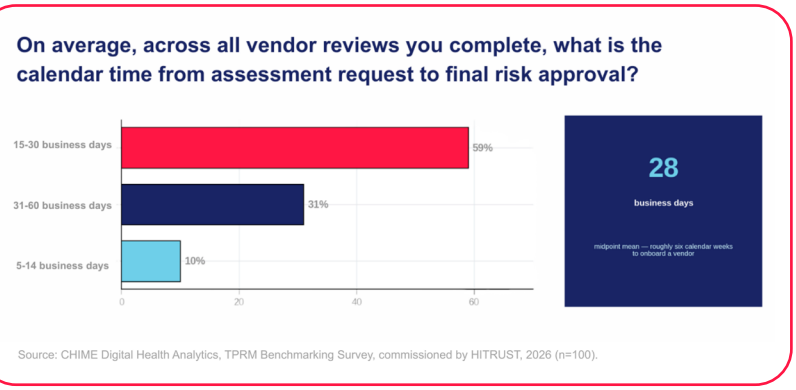
Most assurance mechanisms provide a point-in-time view even when vendor environments continue to change after approval. Services expand, systems change, new downstream providers are introduced, and security incidents alter the risk profile. A review that was reasonable at onboarding might lose relevance before the next scheduled assessment.

Limited monitoring also weakens the organization's response to risk already accepted. A vendor approved with conditions may require enhanced oversight, time-bound remediation, or reassessment when a material event occurs. Without reliable triggers, the exception remains open while the business continues to depend on the service.

> "Modern businesses rely heavily on third-party partnerships to create value and drive innovation, but they are expanding faster than organizations can manage the risks. According to KPMG research, 83 percent of executives plan to expand their partner networks in the next one to three years, yet 71 percent admit that they have trouble getting their partners to align on goals"
>
> **- KPMG 2026 Global Third-Party Risk Management Survey**

What the Evidence Shows

- The CHIME survey found the vendor approval process took a median of 28 days with almost 1/3 taking 31-60 days to complete.



- The Mitratech 2025 Third-Party Risk Management Study[7] reported that only 29% of organizations could assess risk across the full vendor lifecycle, and that organizations actively monitored only 40% of their vendors on average.

What TPRM Leaders Can Do

- Set monitoring depth and reassessment frequency according to vendor risk and operational criticality.
- Trigger reassessment when service scope, system access, data handling, control ownership, or downstream dependencies materially change.
- Connect incident intelligence, remediation status, and monitoring data to the original approval decision.
- Apply enhanced monitoring and clear escalation paths to vendors operating under approved exceptions.

Continuous oversight does not require the same intensity for every vendor. It requires enough risk-based monitoring to recognize when the facts behind an earlier decision have changed.

CLOSING PERSPECTIVE

The challenges described in this report are not isolated weaknesses.

They are interconnected symptoms of a TPRM operating model struggling to keep pace with complexity of modern vendor ecosystems:

- Insufficient staffing and technology limit capacity
- Unreliable assurance creates additional review work
- Business dependencies pressure organizations to accept risks they do not fully understand or cannot adequately mitigate
- Manual processes consume scarce capacity
- Incomplete vendor data undermines risk visibility
- Limited supply chain visibility obscures material exposures

Solving these challenges will require more than incremental improvements to existing processes. Organizations need a more scalable, risk-based model built on complete vendor data, standardized and independently validated assurance, greater automation, and deeper supply chain visibility. The objective is to develop sufficient confidence to identify material exposures early, focus expertise where it matters most, and make timely and defensible decisions.

The organizations best positioned for the future will be those that treat TPRM as an enterprise risk capability. By modernizing vendor assurance, TPRM programs can reduce friction while improving visibility and confidence. Ultimately, the goal is a program that can scale alongside the business without sacrificing the rigor needed to protect critical operations and data.

Methodology and Inputs

Research design

In July 2026, HITRUST commissioned CHIME Digital Health Analytics to conduct a blinded market-validation survey of 102 qualified respondents from separate healthcare provider organizations with more than $1 billion in annual revenue. Respondents represented security and GRC leadership, TPRM ownership, procurement and vendor management, legal and contracting, and executive leadership. Every participating organization actively managed at least 200 third-party vendors, and 87% managed more than 500 vendors.

Qualitative input

The survey findings were supplemented by conversations between HITRUST and TPRM leaders in 2026. Those discussions added practical context on vendor volume, staffing constraints, assessment backlogs, fourth-party visibility, and business pressure. Although the quantitative evidence comes from large healthcare organizations, the operating issues apply broadly to organizations managing complex external ecosystems.

How the Top 10 was developed

The ten issues were developed by synthesizing three inputs: market commentary and external research, direct feedback from TPRM leaders, and HITRUST's commissioned market-validation study. The report distills broad practitioner evidence and community priorities into a concise awareness document that helps leaders focus attention and action. The list is not intended to suggest that every organization experiences every issue equally or that the issues are ranked by a single universal severity score.

Footnotes

[1] 2026 Verizon Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/

[2] World Economic Forum Global Cybersecurity Outlook 2025 - https://www.weforum.org/press/2025/01/global-cybersecurity-outlook-2025-navigating-through-rising-cyber-complexities/

[3] KPMG 2026 Global TPRM Survey - https://kpmg.com/xx/en/our-insights/risk-and-regulation/the-2026-kpmg-global-third-party-risk-management-survey.html

[4] CHIME Digital Health Analytics. Third-Party Risk Management Assurance: Strategic Market Validation Survey. Commissioned by HITRUST. Ann Arbor, MI: College of Healthcare Information Management Executives, Digital Health Analytics 2026. Survey of 102 senior healthcare leaders at U.S. provider organizations with annual revenue of $1 billion or more, fielded June 2026.

[5] Venminder State of Third Party Risk Management 2025 - https://www.venminder.com/hubfs/Venminder_-_State_of_Third_Party_Risk_Management_2025.pdf

[6] Ncontract_State of Third Party Risk Management 2026 - https://www.ncontracts.com/hubfs/ALL Content/Reports/Ncontract_-_state_of_third_party_risk_management_2026.pdf

[7] Mitratech Study Finds TPRM Ecosystems Under Strain - https://mitratech.com/resource-hub/pressreleases/new-mitratech-study-finds-third-party-risk-management-ecosystems-under-strain/

[8] 2026 Study from Panorays: 85% of CISOs Can't See Third-Party Threats Amid Increasing Supply Chain Attacks | GCS Network - https://globalcybersecuritynetwork.com/blog/panorays-ciso-survey-third-party-cyber-risk-management/

[9] World Economic Forum Global Cybersecurity Outlook 2025 - https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

[10] 2023 EY Global Third-Party Risk Management Survey - https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/risk/documents/ey-global-third-party-risk-management-survey-v3.pdf