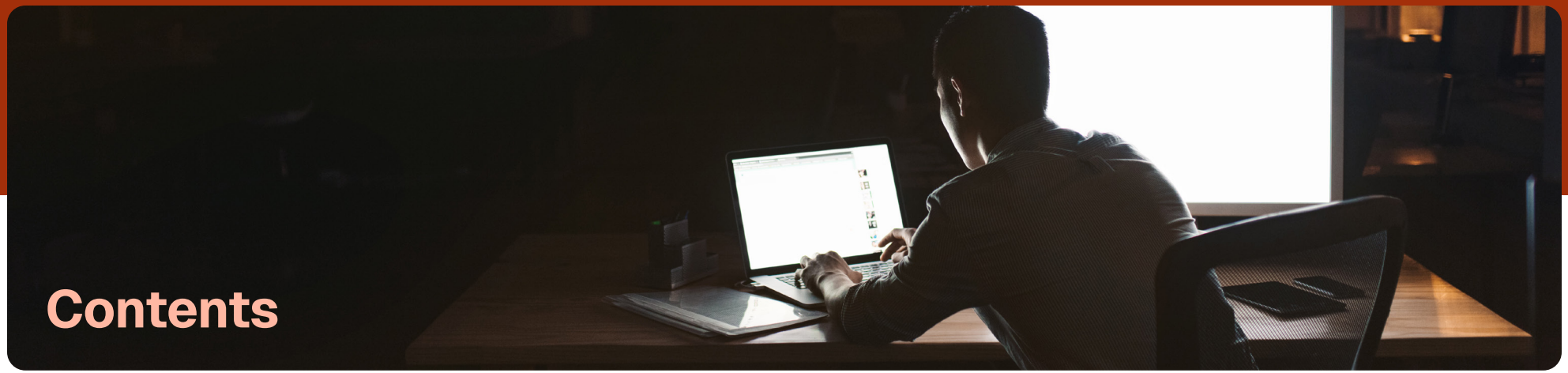
The Roadmap to Modern TPRM

The 4 Stages to Supply Chain Resilience

How to Move Beyond Annual Assessments and Build a Continuous, Threat-Informed TPRM Program

©2026 SecurityScorecard Inc. All rights reserved.



Contents

©2026 SecurityScorecard Inc. All rights reserved.

Why Annual Vendor Risk Assessments Are Failing in 2026

Most organizations believe they are managing third-party risk. They have questionnaires. They have policies in place. They have annual reviews and board decks. They may even have an established culture of cybersecurity resilience.

Yet breaches continue to come through vendors. According to SecurityScorecard's Global Third-Party Breach report, over 35% of breaches now come from a third party.

The uncomfortable truth is that annual assessments **miss 364 days of risk.**

Traditional third-party risk management (TPRM) programs were built for a slower era, one defined by procurement cycles, static data, and point-in-time compliance. But supply chains in 2026 are constantly growing and shifting. A vendor can change cloud providers, introduce a vulnerable dependency, expose credentials, suffer a ransomware intrusion, or otherwise degrade its security posture immediately after the last security questionnaire.

Business teams adopt AI tools before procurement or governance frameworks can catch up. Nth-party dependencies create exposure several layers beyond the vendors most organizations think they are monitoring. At the same time, the distance between threat ideation and threat execution has narrowed. Adversaries can build, test, launch, and pivot in hours.

In that environment, self-reported questionnaires are not enough, and static ratings alone age almost immediately. A document can still be technically accurate and still fail to tell you what matters most right now: whether a supplier's posture is changing, whether an active threat is taking shape, whether a critical vulnerability affects your ecosystem today, and whether your team can act fast enough to contain the impact.

That is why the future of TPRM is moving toward a continuous, threat-informed model shaped by live telemetry, broader context, faster validation, and measurable risk reduction. A modern program should help you continuously manage, detect, prioritize, and drive down third-party risk. It should help your team spend less time collecting evidence and more time making defensible decisions. It should also give leaders a clearer answer to the question that boards, regulators, and customers increasingly ask: are we reducing risk in a way we can prove?

This ebook is about one central question. What should you expect from a modern TPRM program in 2026, and what are you missing if your current model still depends on stale snapshots of a fast-moving ecosystem?

> *"The biggest blind spot is the lack of coordination and communication between us and our different suppliers... Sometimes I feel overwhelmed with the large amount of vendors we have."*
>
> SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report

©2026 SecurityScorecard Inc. All rights reserved.

What Happens When TPRM Stays Reactive in 2026

MANY ORGANIZATIONS ARE STUCK IN ONE OF THREE PATTERNS:

- Compliance-first assessments without operational follow-through
- Manual workflows that exhaust teams
- Monitoring without actionable context

THIS RESULTS IN:

- Invisibility between annual reviews
- No unified threat context across vendors
- Difficulty proving measurable risk reduction to the board
- Alert fatigue without prioritization

55% OF ORGANIZATIONS

still rely on manual methods, such as calls, meetings, emails, or collaboration with points of contact, to conduct outreach to vendors when a breach occurs, according to data from a 2026 survey firm unreal.

SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report

Many organizations have not ignored third-party risk. They have simply inherited a model that no longer matches the problem. Their teams work hard, their processes are documented, and their intent is sound. What holds them back is not a lack of effort. It is the growing mismatch between point-in-time governance and an always-changing attack surface.

For some teams, the burden shows up as endless questionnaire follow-up and evidence collection. For others, it appears as fragmented monitoring that produces signals without helping anyone decide what matters. In more mature environments, the issues may be less obvious: risk data exists, yet the organization still cannot connect vendor posture, threat activity, and business impact quickly enough to act with confidence.

That is why there is no single starting point for modernization. Organizations differ in size, industry, regulatory burden, operating model, and internal maturity. Some are constrained by spreadsheets. Some by process debt. Some by tooling that offers visibility without action. Some by security programs that remain separated from procurement, legal, vulnerability management, and executive reporting.

What unites them is the cost of delay. Between formal review cycles, risk accumulates quietly. Critical vendors change. Exposure spreads into fourth parties and beyond. A new zero-day appears and the organization cannot determine impact without launching a manual exercise across multiple teams. The board asks whether risk is going down, and the answer depends on static reports rather than current reality.

You're not failing due to negligence. You're constrained by outdated models. Teams are busy, but not always advancing. Leaders are accountable, but not always equipped with the right evidence. The result is a program that may look mature from a distance while still leaving the organization exposed at the moments that matter most.

©2026 SecurityScorecard Inc. All rights reserved.

What Are the 4 Stages of Third-Party Risk Management Maturity?

Every organization is at a different point on the maturity curve, and that position is shaped by more than budget or company size. A large enterprise can still run a fragmented, spreadsheet-heavy vendor program. A smaller but highly disciplined organization can build a more modern operating model because it has clear ownership, better workflows, and stronger integration between security and business functions.

Maturity is really a measure of how well your program keeps pace with change. It reflects whether your team can see the ecosystem clearly, whether it can validate what vendors say, whether it can prioritize threats with context, and whether it can turn findings into timely action.

©2026 SecurityScorecard Inc. All rights reserved.

Stage 1

Basic Diligence

Current State

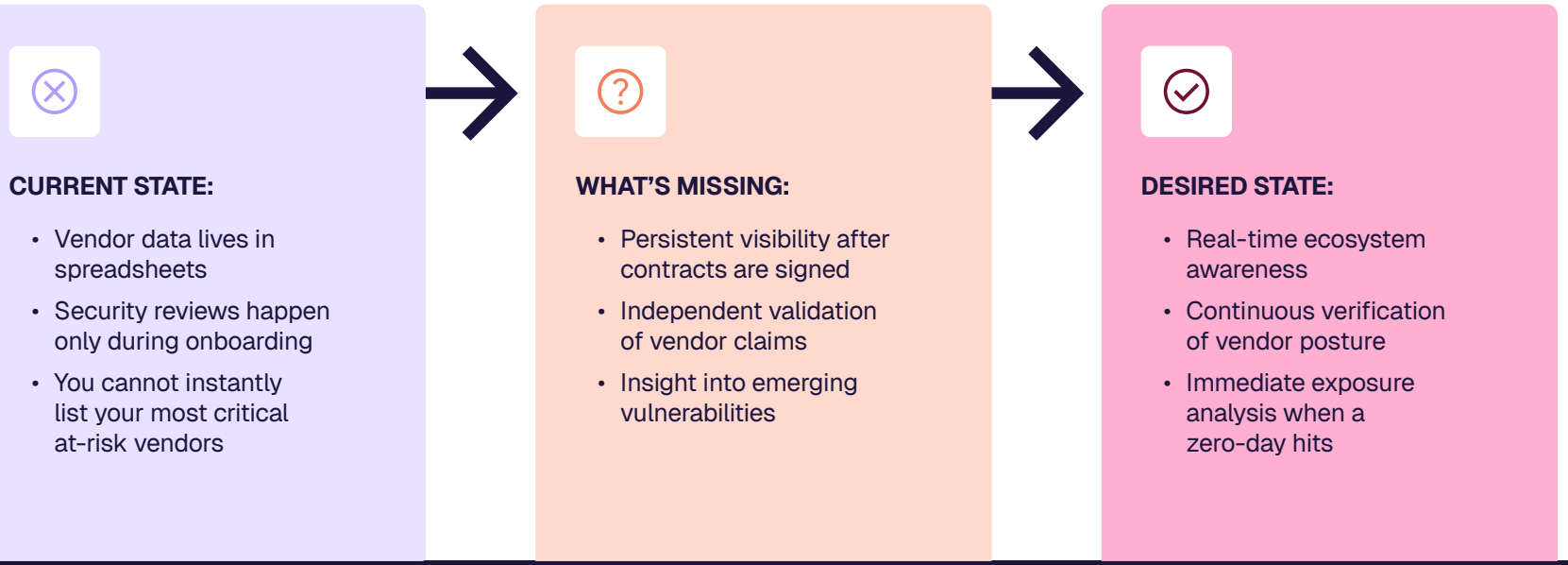
At the basic diligence stage, third-party reviews are usually tied closely to procurement. A vendor is assessed during onboarding, documentation is collected, and the review is filed away once the contract is signed. The program may be thoughtful and conscientious, but it is still largely episodic.

A team at this stage often knows that it has gaps. Vendor data may live in Excel, a shared drive, or a flat procurement database. Security reviews are often treated as a one-time hurdle for new contracts. If leadership asks for a current list of the most critical at-risk vendors, it can take time to assemble and validate the answer.

What is missing here is not only visibility. It is confidence. Teams can work hard and still feel that risk becomes opaque the moment a vendor enters production. They know a review was completed, but they do not know how much has changed since then, what hidden dependencies sit behind the supplier, or whether emerging threats are already affecting the ecosystem.

Desired State

The next step is not simply more assessments. It is a better ability to maintain awareness after onboarding. That means continuous knowledge of who is in your supply chain, external validation of vendor claims, and faster exposure analysis
when a zero-day or major incident breaks. The future state for these teams is a program that keeps working after the contract is signed.



©2026 SecurityScorecard Inc. All rights reserved.

Stage 2

Periodic TPRM

Periodic TPRM reflects a meaningful step forward. Policies are established, workflows are standardized, and there is usually a dedicated team or a clearer operating rhythm. Assessments may occur annually, bi-annually, or quarterly for the most critical vendors. There is a stronger culture of risk management, and the organization has moved beyond ad hoc diligence.

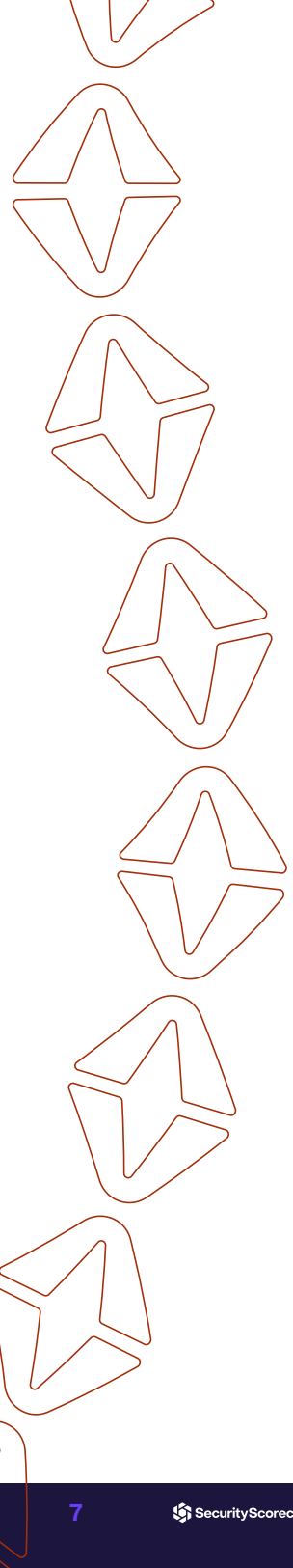
Current State

Still, the model remains anchored to intervals. Teams spend too much time chasing questionnaire responses, validating documentation manually, and working through backlogs that are already aging by the time they are reviewed. A program can be organized and still remain vulnerable to drift between assessment cycles.

Teams have invested in process maturity, yet they still feel captive to admin-heavy work. Security leaders know the data is dated. Business stakeholders want faster answers. The program generates activity, but not always the level of assurance the organization expects.

Desired State

The way forward is to move beyond calendar-based awareness. Continuous alerts for posture changes, integrated threat intelligence that adds real context to vendor profiles, and more efficient workflows can materially change how teams operate. Freeing up even a large portion of the manual workload can reshape the program. It gives skilled practitioners time to focus on high-impact decisions, vendor engagement, and risk reduction rather than inbox management and evidence wrangling.



CURRENT STATE:

- Assessments are annual, bi-annual, or quarterly
- Teams spend most of their time chasing questionnaires
- Risk snapshots are outdated by the time they're reviewed

WHAT'S MISSING:

- Detection of posture changes between reviews
- Threat context layered onto vendor data
- Automation to reduce manual follow-up

DESIRED STATE:

- Automated posture change alerts
- Integrated threat intelligence fused with vendor profiles
- Reduced manual workload by up to 95%

©2026 SecurityScorecard Inc. All rights reserved.

Stage 3

Continuous TPRM

At the continuous stage, the program begins to behave more like a living system. Teams receive alerts when vendor posture changes. They validate questionnaire answers with external telemetry. They can respond faster when a major vulnerability or active incident emerges.

Current State

This is a significant advance, but it does not automatically solve prioritization. Continuous monitoring can still overwhelm teams if the data lacks business context or if external signals are not tied clearly to internal exposure and vendor criticality. A risk finding matters differently when it affects a niche tool than when it affects a concentration point in your financial systems, healthcare operations, or customer-facing infrastructure.

That is the core challenge at this stage. Many organizations can see more, but they still need stronger ways to interpret what they are seeing. The most useful next capability is richer context: which threats are active, which vendors are materially exposed, what part of the business is implicated, how remediation should be sequenced, and who needs to act first.

Desired State

Continuous monitoring creates value only if it can drive a response. Teams need workflows that help them communicate with suppliers clearly, track progress, document remediation, and escalate where necessary. Otherwise, the program surfaces more risk without increasing the organization's ability to reduce it.

©2026 SecurityScorecard Inc. All rights reserved.

Stage 4

Threat-Informed TPRM

Desired State

At the most mature stage, the program develops operational depth. Threat intelligence informs prioritization directly. Teams are no longer waiting for annual reviews or relying on generalized findings to decide where to focus. They know which exposures matter because they understand who is being targeted, how active threats are evolving, and where the business is most vulnerable.

Here, the organization monitors the ecosystem continuously and interprets that activity through live threat context. Analysts use telemetry and intelligence to separate background noise from credible operational risk. Cyber, GRC, vulnerability management, and business stakeholders work from a more shared understanding of what matters and why. Vendor communication becomes more purposeful because it is informed by evidence, timing, and impact.

Reporting also changes. Instead of presenting counts of completed reviews or overdue questionnaires, leaders can describe exposure trends, concentration risk, remediation velocity, and the likely impact of unresolved issues. The program becomes more defensible to boards and regulators because it is closer to reality.

This is the stage at which TPRM begins to support resilience as an operating capability. The organization is not only reviewing vendors. It is managing an ecosystem with greater precision, stronger evidence, and better timing. This is where TPRM becomes an operational defense capability rather than a compliance exercise meant to “check-the-box.”

AT THIS STAGE:

- Your team integrates real-time threat intelligence with vendor risk data
- Security, GRC, and SecOps teams operate from shared supply chain intelligence
- Vendor exposure to active threats can be identified quickly
- Supplier engagement begins as risks emerge, not only after incidents

©2026 SecurityScorecard Inc. All rights reserved.

What Is Your TPRM Program Missing?

Many programs contain parts of a modern model without yet delivering the full outcome. That is why maturity should be assessed through capabilities, not labels.

A strong 2026 program should be able to validate vendor claims continuously with live external intelligence rather than relying only on self-attestation. It should be able to connect external threat activity to supplier exposure, not merely display posture data in isolation. It should reduce dependence on manual outreach by giving teams more structured ways to engage vendors and track remediation.

It should also help teams prioritize better. That means filtering noise, elevating high-consequence exposures, and showing which issues are likely to matter in practice. It should give executives a clearer view of whether risk is rising, stabilizing, or declining over time. And it should strengthen coordination across teams that have historically worked from different systems and different assumptions.

If any of these are missing, the program may still be functioning, but it is likely functioning with only partial visibility and partial control.

©2026 SecurityScorecard Inc. All rights reserved.

10 The THINGS Your TPRM Program Needs in 2026

1 CONTINUOUS VERIFICATION

Vendor claims validated continuously with independent external intelligence rather than relying solely on self-reported questionnaires or periodic reviews.

2 UNIFIED THREAT CONTEXT

Threat intelligence connected directly to vendor risk data so teams can identify which suppliers are exposed to active threats, exploited vulnerabilities, or emerging attack campaigns.

3 AUTOMATED VENDOR ENGAGEMENT

Structured workflows that replace fragmented follow-ups and help teams coordinate remediation, track vendor responses, and resolve issues faster.

4 RISK-BASED PRIORITIZATION

Clear prioritization that focuses attention on exploitable risks and business-critical vendor exposures rather than alert volume alone.

5 AI-DRIVEN RISK MANAGEMENT

AI-assisted workflows that reduce manual effort and help teams analyze vendor risk faster, prioritize what matters, and conduct more consistent assessments at scale.

6 PREDICTIVE RISK AWARENESS

Early signals that help teams identify where supply chain risk is forming so action can be taken before incidents impact the business.

7 RAPID EXPOSURE ANALYSIS

The ability to quickly determine which vendors are affected when new vulnerabilities, threat campaigns, or major incidents emerge.

8 MEASURABLE RISK REDUCTION

Clear evidence that vendor security posture and overall ecosystem risk are improving over time rather than simply tracking completed assessments.

9 CROSS-TEAM INTELLIGENCE SHARING

Cybersecurity, GRC, vulnerability management, and threat intelligence teams operate from shared supply chain intelligence instead of fragmented tools and data sources.

10 BOARD-READY METRICS

Executive reporting that translates vendor risk into measurable exposure trends, enabling clear conversations with boards, regulators, and leadership.

©2026 SecurityScorecard Inc. All rights reserved.

Why Modernizing TPRM Matters More in 2026

In 2026, the case for modernization is no longer abstract. Third-party risk is not a secondary issue sitting alongside core security concerns. It is one of the principal ways those concerns materialize.

SecurityScorecard's research shows that more than one-third of breaches originate with third parties. And that number is rising. The Verizon Data Breach Investigations Report likewise found a sharp rise in breaches involving third parties, with the share doubling from 15% to 30% in a single year. File-sharing software became the most common third-party attack vector. More than 41% of ransomware breaches now have roots in third parties.

These numbers reveal a change in attacker logic. Adversaries increasingly look for leverage. If one supplier gives them access to dozens of downstream organizations, that supplier becomes a high-efficiency target. The attack surface is no longer limited to the systems an enterprise directly owns. It extends through SaaS providers, software libraries, outsourced services, cloud infrastructure, file transfer tools, and the hidden interconnections among them.

This is why preparation in 2026 requires more than good internal controls. Organizations need a clearer understanding of which suppliers matter, where exposure is concentrated, how quickly the ecosystem can be assessed during a major event, and whether vendor-related risk can be reduced before an incident spreads into business disruption.

> *"Third-party involvement in breaches was an ever-present subject in incidents throughout this past year. Third parties not only act as custodians to customers' data, but they also underpin critical parts of organizations' operations."*
>
> Verizon Data Breach Investigations Report

©2026 SecurityScorecard Inc. All rights reserved.

Why Unified Threat Intelligence Matters for Third-Party Risk Management

Continuous monitoring generates value, but only when it is paired with context. Otherwise, teams inherit the familiar burden of modern security operations: a growing stream of alerts without a reliable way to distinguish meaningful threats.

Unified threat intelligence addresses that problem by connecting vendor posture to the external environment in which adversaries operate. It brings together attack surface data, vulnerability telemetry, leaked credential monitoring, malware indicators, exploit chatter, observed adversary behavior, vendor-provided attestations, and assessment data. Instead of treating these as separate views, it makes them part of one risk picture.

That matters because threat-informed TPRM is not just a more technical version of monitoring. It is a more discriminating one. A critical vulnerability is important. A critical vulnerability that is being actively exploited, affecting a strategic vendor, and tied to a concentration point in your ecosystem is urgent in a different way. Threat intelligence helps teams understand that difference and act accordingly.

It also improves trust in the program itself. When findings are supported by rich external evidence and grounded in real-world threat activity, vendor conversations become more concrete, internal escalation becomes easier, and leadership reporting becomes more persuasive. In practice, that is what it means to be threat-informed: seeing risk through the lens of relevance, timing, and consequence.

©2026 SecurityScorecard Inc. All rights reserved.

Why Manual Security Questionnaires No Longer Keep Pace With Modern Threats

Security questionnaires were designed for a slower risk environment. They assumed that vendor security posture changed gradually and that a periodic snapshot could provide a reliable view of risk. In 2026, that assumption no longer holds.

Supply chains now evolve continuously. Vendors deploy new code daily, adopt new infrastructure providers, introduce new dependencies, and expand their digital footprint across multiple environments. At the same time, attackers move faster than ever. When a new vulnerability or exploit appears, adversaries can begin targeting exposed systems within hours. A questionnaire completed six months ago—or even six weeks ago—cannot capture that reality.

This is where the manual model begins to break down. Questionnaires take time to send, complete, review, and validate. By the time responses arrive, the environment they describe may already have changed. Teams are left comparing documents rather than understanding current exposure. Even the most diligent programs struggle to keep pace when risk signals are arriving faster than documentation cycles.

Manual collection also creates operational drag. Vendors face repeated requests from different customers, often asking for the same information in slightly different formats. Internal teams spend valuable time chasing responses, validating evidence, and reconciling spreadsheets. Instead of focusing on the vendors and vulnerabilities that present real operational risk, skilled practitioners are pulled into administrative work.

64% OF RESPONDENTS

in a 2026 unreal survey attested that under **50% of their vendors comply with their internal rules,** leaving gaps in visibility and security.

SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report

©2026 SecurityScorecard Inc. All rights reserved.

Why Manual Security Questionnaires No Longer Keep Pace With Modern Threats (continued)

How AI is influencing Modern TRPM Programs

Modern TPRM programs are beginning to move away from this document-first model toward verification-first workflows. Questionnaires still play an important role in capturing governance practices, policies, and controls. But they are increasingly complemented by continuous intelligence that validates vendor claims and highlights changes in security posture between review cycles.

Updating traditional assessments with real-time visibility and AI-driven workflows form the basis of a TPRM process that reflects how risk actually evolves. Security ratings provide an independent baseline view of vendor security posture and track changes over time. AI-driven workflows streamline the exchange and validation of security materials. **For organizations that need additional operational capacity, managed support can help identify high-risk suppliers, monitor active threats across the vendor ecosystem, and coordinate remediation efforts more efficiently.**

With this new approach, assessments become easier to complete and easier to verify. Vendors spend less time responding to duplicative requests. Internal teams gain faster insight into which suppliers require attention and why.

When assessments are supported by continuous intelligence rather than replaced by it, the program becomes more responsive to the speed of modern threats. Organizations can maintain documentation for compliance while also gaining the visibility and context needed to manage risk in real time.

©2026 SecurityScorecard Inc. All rights reserved.

How To Address The Unique TPRM Priorities of 6 Key Stakeholders in Your Ecosystem

A modern TPRM program has to resonate across the organization because third-party risk is felt differently depending on where you sit.

©2026 SecurityScorecard Inc. All rights reserved.

The Enterprise CISO

For the Enterprise CISO, the pressure is strategic and visible.

Boards want proof that supplier risk is understood and controlled. Regulators expect defensible governance. The business needs confidence that vendor exposure is not eroding resilience. Better looks like executive reporting that shows quantified trends, clearer peer context, and a stronger narrative linking third-party risk to business continuity and risk reduction. The possibility here is composure. The CISO can speak with more authority because the program provides current evidence rather than retrospective assurance.

CHALLENGES

- Proving risk reduction to the board
- Translating vendor risk into business impact
- Navigating regulatory scrutiny

WHAT BETTER LOOKS LIKE

- Executive dashboards with quantified exposure trends
- Peer benchmarking and competitive posture analysis
- Clear, defensible narratives for regulatory conversations

©2026 SecurityScorecard Inc. All rights reserved.

The Chief Risk Officer

For the Chief Risk Officer, the challenge is integration.

Third-party cyber risk often sits apart from enterprise risk models, making it difficult to compare, quantify, and govern consistently across the business. Better looks like a program that feeds continuous supplier intelligence into broader dashboards, supports financial impact modeling, and aligns cyber signals with operational resilience. The possibility is a risk function that treats supplier exposure as a measurable enterprise issue rather than a technical appendix.

CHALLENGES

- Fragmented risk visibility across business units
- Inability to quantify third-party exposure
- Difficulty aligning cyber risk to enterprise risk frameworks

WHAT BETTER LOOKS LIKE

- Integrated third-party risk within enterprise dashboards
- Financial impact modeling tied to vendor exposure
- Continuous risk scoring tied to operational resilience

©2026 SecurityScorecard Inc. All rights reserved.

The Chief Revenue Officer

For the Chief Revenue Officer, security friction can surface as business friction.

Vendor assessments delay partnerships. Customer security reviews slow deals. Internal stakeholders experience security as an obstacle to momentum. Better looks like faster validation, more reusable documentation, and clearer trust signals that reduce back-and-forth during commercial cycles. The opportunity is practical: security helps the company move faster because it can answer questions quickly and credibly.

CHALLENGES

- Vendor risk slowing deals
- Security reviews delaying revenue
- Customer security audits overwhelming teams

WHAT BETTER LOOKS LIKE

- Accelerated vendor validation
- Shared security profiles that build trust
- Faster contract approvals through standardized documentation

©2026 SecurityScorecard Inc. All rights reserved.

The TPRM / GRC Leader

For the TPRM or GRC leader, the biggest burden is often operational drag.

Manual workflows, inconsistent vendor responsiveness, and weak remediation tracking consume the team's time. Better looks like a more structured operating model with automated outreach, continuous posture updates, and clearer evidence trails. The reward is not just efficiency. It is a chance to spend more energy on program strategy, priority setting, and stakeholder communication rather than repetitive administration.

CHALLENGES

- Spreadsheet-driven processes
- Vendor responsiveness gaps
- Inconsistent remediation tracking

WHAT BETTER LOOKS LIKE

- Automated outreach and response tracking
- Continuous posture updates without manual chasing
- Audit-ready documentation at any moment

©2026 SecurityScorecard Inc. All rights reserved.

SecOps & Vulnerability Management

For SecOps and vulnerability leaders, the issue is incomplete sight.

Internal assets may be well covered, while third-party exposures remain harder to map and harder to prioritize. Better looks like continuous detection of critical vendor exposures, more relevant alerting based on exploitability and business dependence, and cleaner integration into existing SOC and SIEM processes. The gain is sharper signal quality and faster decision-making when time matters.

CHALLENGES

- Vulnerability overload
- Third-party blind spots
- Disconnected internal and vendor intelligence

WHAT BETTER LOOKS LIKE

- Continuous visibility into vendor exposure when critical vulnerabilities or zero-days emerge
- Prioritized alerts based on exploit likelihood
- Integrated workflows into existing SIEM and SOC tooling

©2026 SecurityScorecard Inc. All rights reserved.

Threat Intelligence Teams

For threat intelligence teams, the problem is often one of linkage.

They may have high-value external intelligence, but limited ways to map it to supplier ecosystems or convert it into business action. Better looks like direct connection between adversary activity and the vendors that support key operations, along with stronger coordination with GRC and security functions. The result is a threat intelligence discipline that contributes not only to awareness, but to prevention.

CHALLENGES

- Signals without vendor mapping
- Inability to connect external threats to supplier exposure
- Lack of coordination with GRC

WHAT BETTER LOOKS LIKE

- Direct linkage between threat actors and vendor ecosystems
- AI correlation of high-risk attack paths
- Shared intelligence layer across cyber and compliance

©2026 SecurityScorecard Inc. All rights reserved.

TPRM SELF-ASSESSMENT

6 Questions to Ask Before Your Next Vendor Incident

A useful way to assess your current maturity is to ask a few direct questions.

If these questions remain difficult to answer, that's a good indicator that a TPRM program may be functioning but overdue for a change.

- **Can your team validate vendor claims without relying entirely on self-reporting?**
- **Can you identify the most critical at-risk vendors in minutes rather than days?**
- **Can you determine which suppliers are exposed to a new vulnerability today?**
- **Can you show how third-party risk is trending over time, not just how many assessments were completed last quarter?**
- **Are questionnaires slowing customer deals, vendor onboarding, or internal decision-making?**
- **When the board asks whether the program is reducing risk, do you have trend lines and evidence or only snapshots?**

©2026 SecurityScorecard Inc. All rights reserved.

How to Modernize Third-Party Risk Management Before the Next Incident

Modern TPRM should strengthen the expertise your team already has and help it perform under real conditions. It should provide a more continuous understanding of the ecosystem, bring threat context into daily prioritization, and reduce the manual burden that keeps experienced people trapped in administrative work. It should give leaders stronger evidence, vendors clearer expectations, and the organization a more believable path toward resilience.

SecurityScorecard has helped over 3,300 organizations, including 70% of the Fortune 100, evolve their third-party programs with continuous visibility, industry-leading security ratings, threat-informed intelligence, workflow support, and managed services such as MAX for teams that need additional operational capacity. The work is grounded in a simple recognition: organizations are at different stages, and modernization succeeds when it builds on the structure they already have.

SecurityScorecard supports organizations at every stage of this maturity curve, whether rooted in basic diligence, periodic reviews, or already automated workflows. By integrating continuous telemetry, unified threat intelligence, and streamlined vendor collaboration, teams move from documentation management toward demonstrable resilience.

Teams that once felt behind can begin to feel ready. Leaders who once relied on stale reports can begin to speak from current evidence. Risk programs that once lived in the background can become more central to resilience, governance, and growth.

The organizations that make this shift in 2026 will be better prepared to move with the speed of the business and the speed of the threat landscape. They will have a clearer view of their suppliers, stronger ways to verify trust, and better confidence in the decisions they make when risk begins to rise.

Modern TPRM provides continuous awareness, unified intelligence, measurable outcomes, and collaborative remediation. Anything less leaves exposure accumulating between review cycles.

By fusing continuous intelligence, AI-accelerated workflows, and streamlined vendor engagement, teams move from defensive bottlenecks to confident leaders of supply chain resilience.

A practical next step is to see your current ecosystem through a more continuous lens. Request a free demo, schedule a conversation with a SecurityScorecard expert, or explore how security ratings, managed services through MAX, and streamlined documentation workflows can help your team modernize at its own pace.

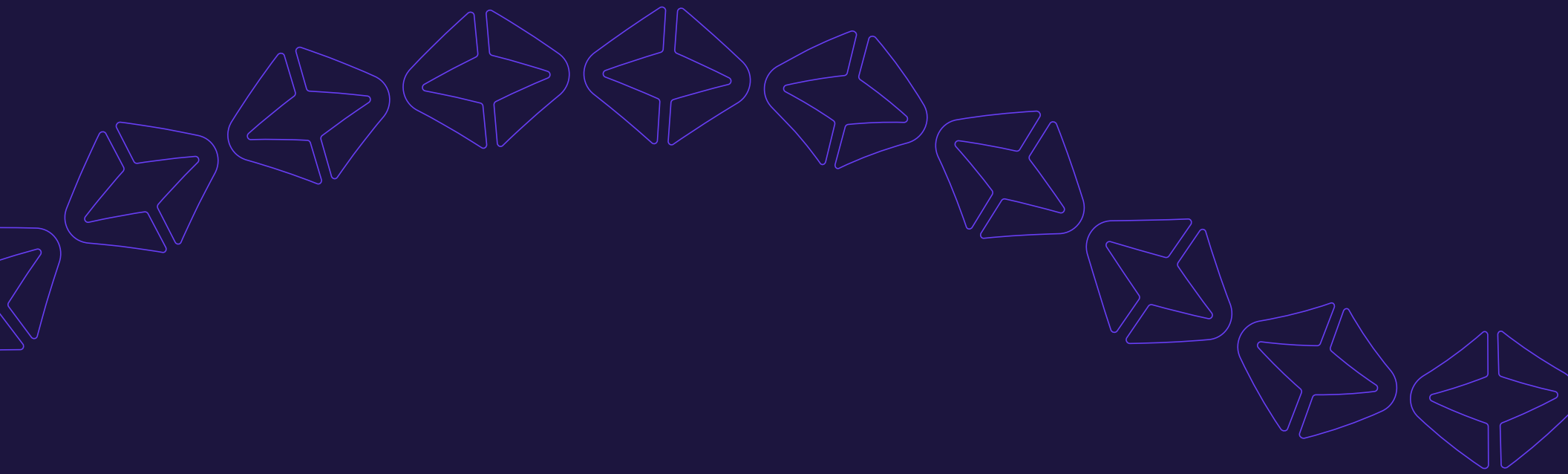
©2026 SecurityScorecard Inc. All rights reserved.

About SecurityScorecard

SecurityScorecard is the global leader in threat-informed third-party risk management (TPRM), securing the world's supply chains. The company delivers a modern, threat-informed approach to TPRM that enables organizations to drive out risk at the source. Through continuous visibility, AI-accelerated workflows, and predictive insights, the platform transforms third-party risk into a competitive advantage, empowering organizations to proactively reduce risk before incidents occur and respond with confidence when they do, delivering measurable supply chain resilience.

Trusted by over 3,300 organizations, including 70% of the Fortune 100, and recognized as a trusted resource by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, Google Ventures, NGP Capital, Intel Capital, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity.

Protect the supply chain behind your business. Learn more at securityscorecard.com.



SecurityScorecard

©2026 SecurityScorecard Inc. All rights reserved.