5 Proven Strategies to Maximize Supply Chain Cyber Risk Management

BITSIGHT

Table of Contents

01

The Need for Integrated TPRM to Protect The Supply Chain

01 The Need for Integrated Third-Party Risk Management to Protect The Supply Chain

Simplify, integrate, consolidate... CISOs are experiencing top-down pressure to optimize and demonstrate the value of their operations and security programs, as well as tools and resources. They are often tasked to reduce costs, consolidate vendors or do more with no further increase in staff or budget—whilst a high expectation of protecting their organization from cyber threats continues.

Tim Grieveson
Senior Vice President—
Global Cyber Risk Advisor, Bitsight

Four reasons why this is adding more pressure than ever:

▶ **The digital supply chain is booming,** but the tools and processes in place to assess and reduce vendor risk often don't scale as fast. This is fueled by the increased dependency on SaaS applications, whether known or unknown—with Shadow IT creating additional blindspots.

▶ **Third-party breaches are on the rise,** and they're costing big time. SolarWinds, Kaseya, and MOVEit zero-day vulnerabilities were wake-up calls, reminding us that bad actors love nothing more than a backdoor into your network via a vulnerable vendor.

▶ **Regulations are increasing expectations**—from the SEC requirements in the US to DORA and NIS2 frameworks in the EU, the compliance landscape is getting tighter by the minute. Cybersecurity leaders are facing increased accountability, customers are demanding trust, and boards and regulators are cracking down harder on supply chain resilience.

▶ **The adoption of AI and ML continues to surge,** boosting technology use for good—like AI-enhanced threat hunting —but also risking weaponization by threat actors, such as ransomware as a service campaigns. With more automated and complex use cases, there is a potential to unintentionally increase attack surfaces with unapproved and unreviewed applications from a quality and security suitability stand-point. Making technology solutions simpler to develop and available to everyone without specialized IT development or security experience should be carefully considered.

So how can you be more resourceful as you look to maintain a best-in-class cyber risk management program and continue to meet business expectations?

This is your guide to building efficient, scalable, and repeatable Vendor Risk Management (VRM) workflows as part of your holistic Third-Party Risk Management (TPRM) program — one that is integrated and continuously detects, monitors, and mitigates vendor risk. We're talking going beyond initial assessments and moving toward proactive, continuous monitoring of vendor health, validating 'yes/no questions' with objective data, and utilizing a collaborative approach to speed up response and remediation activities — which is essential for emerging regulations — all the while speaking the universal language of positive business outcomes.

The strategies in this ebook will allow you to consolidate solutions so your program can grow with the business — managing hundreds or even thousands of vendors as effectively as it manages ten. If you're serious about cybersecurity, this is your chance to take the pivotal step towards end-to-end third-party risk management and accelerate your supply chain programs to comply with the requirements of regulations such as SEC, NIS2, or DORA.

02

Expanding TPRM To Enable Business Outcomes

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Expanding Third-Party Risk Management to Enable Business Outcomes

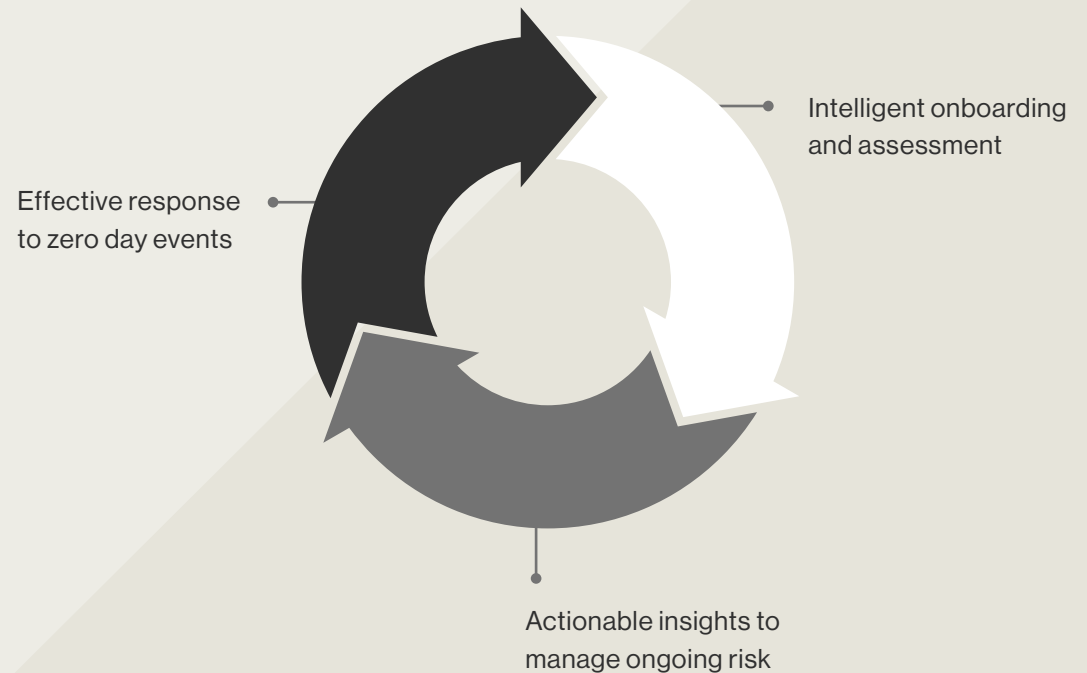**02**

02 Expanding TPRM To Enable Business Outcomes

Cybersecurity professionals are constantly bombarded with an ever-evolving risk and regulations landscape. Finding tools and processes that work, and sticking to them, help security leaders stay consistent.

Adopting a holistic, integrated approach to Third-Party Risk Management (TPRM) is a strategy your organization will only benefit from over the course of your relationships with your vendors as you build a program that proves its value and business outcomes.

Centralizing and combining vendor onboarding with a single, wider view into your risk portfolio, and capabilities to rapidly detect and respond to emerging security events and zero days, shrinks exposure through better, systemic workflows.

▶ Instead of switching between spreadsheets and apps, security managers can increase visibility and efficiency by consolidating these TPRM functions to the right.

End-to-End Third-Party Risk Management

Intelligent onboarding and assessment

Effective response to zero day events

Actionable insights to manage ongoing risk

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Expanding Third-Party Risk Management to Enable Business Outcomes

02

Why The Typical Approach to TPRM is Failing

For a long time, questionnaires were one of the only ways to gather IT security information about third-party vendors. This would force security managers to base their third-party risk management decisions on subjective data and responses, with little visibility into critical external vulnerability data like on-premise controls, SIEMs, firewalls, Shadow IT, remote networks, subsidiaries, or cloud data.

But these manual, one-off spreadsheets with dozens or hundreds of questions, multiple email follow-ups, and calendar reminders are error-prone, unscalable, and ineffective at reducing risk. Vendors could easily misunderstand a question, mistakenly check the wrong box, or have a lack of knowledge about their controls, policies, and procedures.

This approach fails to address and mitigate ongoing risk, offering poor visibility over the evolving third-party risk landscape and emerging zero day vulnerabilities.

▶ A risk assessment is a snapshot of a vendor's security posture, but how can you be sure everything stays the same until your next reassessment?

Threats now happen faster and at greater scale, but it can be challenging to prioritize and visualize risk holistically across the entire supply chain ecosystem. The expanding regulatory landscape makes it critical for cybersecurity leaders to have a single place to see risk and act on it, ensuring findings are actionable.

Ask yourself:

✓ Can your current workflow scale to manage the ever-increasing vendor portfolio without increasing resources, cost, or complexity to ensure you can capture criticality to your business and alignment to compliance obligations?

✓ Are vendor questionnaire responses, certificates, and self attestations enough evidence or would you benefit from objective data to better understand their security posture over time?

✓ When emerging risks and vulnerabilities are effectively detected, how easy is it to act on them? How many applications do you need to initiate vendor outreach and ensure timely mitigation?

✓ Do you have complete visibility into the entire threat landscape across your digital supply chain, including fourth-party risk, as well as insights and recommendations around the overall health of your ecosystem?

✓ Can you confidently report and communicate the effectiveness of your program, or answer questions from your Board around how much risk was reduced or prevented, or how to financially quantify that risk and correlate it to actual security outcomes?

03

Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

03

03 Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

Vendor Risk Management (VRM) is often a starting point for Third-Party Risk Management (TPRM), streamlining the workflow to assess, manage, and reassess vendors. As a logical next step in the TPRM maturity journey, organizations may add more holistic capabilities, such as continuous monitoring, fourth-party risk management, and vulnerability detection to respond to major security events quickly, thus facilitating effective assurance.

Holistic TPRM increases end-to-end visibility over the digital supply chain, by measuring and continuously monitoring third-party security controls, ultimately aligning the program with your risk tolerance and organizational objectives.

GO FROM…		TO…	
✕	Security requests scattered amongst teams and platforms	✓	A single source of truth, shareable across teams and organizations
✕	Data saved across spreadsheets, emails, and manual questionnaires	✓	All third-party risk data captured and analyzed in one platform
✕	Manual, slow exchanges across weeks, if not months	✓	Real time updates, objective data, and continuous monitoring of the supply chain
✕	Reliance on incomplete or outdated data to make decisions	✓	Reliance on incomplete or outdated data to make decisions

Here is a step-by-step guide for creating a sustainable and scalable third-party risk management program from the ground up.

STEP 1:

Build the foundation for vendor risk assessments and onboarding

Lay the groundwork for standardized procedures and clear criteria for evaluating vendor risk, ensuring consistency and efficiency across your organization.

Typical requirements include:

- Standard questionnaires like SIG Core and Lite, Cloud Security Alliance CAIQ, or CIS Controls.

- Certifications like SOC2 reports, ISO 27001, HiTrust, or Cyber Essentials.

- Attestations such as penetration tests, application scans, or insurance documentation.

- Industry-specific standards such as HIPAA for organizations handling healthcare data, PCI DSS for organizations handling credit card data, NERC CIP for critical infrastructures in the electricity sector, or NIST 800-53, which provides a catalog of security and privacy controls based on risk, cost-effectivness, and capabilities.

- Local regulation standards such as those from the SEC in the US, NIS2 and DORA in the EU, PS21/3 in the UK, or privacy standards like GDPR or CCPA.

Managing vendor relations needs to be a collaborative effort between vendor relationship owners, security, legal, procurement, compliance, accounting, and other departments. As you develop your program, involve those members of your organization whose contributions and participation are critical, and establish a mutually agreed-upon foundation. Focus on demonstrating how a relatively modest investment can result in a substantial reduction of annual loss expectancy from third-party risk.

Finally, select the providers you will use to build and automate your process. Take the time to thoroughly research TPRM tools, and look for those who offer an end-to-end solution that goes beyond questionnaires and due diligence, incorporating objective analytics and data to help you make better decisions.

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

03

STEP 2:

Set up automated workflows for reassessment, continuous monitoring, and vulnerability exposure

Embrace automation to keep pace with your ever-growing vendor ecosystem and the evolving threat landscape. By leveraging continuous monitoring and vulnerability detection technology to proactively identify and address risks in real-time, you can enhance your organization's resilience against cyber threats and keep a constant pulse on vendor security.

When zero day events occur, you need to quickly understand the scope of the problem across your ecosystem and respond. How do you identify which vendors have been impacted? How do you work with them to prioritize mitigation efforts? And what do you tell your board members when they ask for a remediation report?

Your process should focus on areas of risk which could have an immediate impact to your business, for example, compromised systems, or the presence of vulnerabilities and threats that are common to the vendor's industry. Establish a periodic reassessment cadence based on risk level—you may often want to reengage third parties outside your normal cadence in the case of a security incident or breach, a zero-day vulnerability made public, or after you've updated your risk thresholds.

Vendor Reassessment Cadence Example

RISK TIER	CONTRACT REVIEW	RISK CATEGORIZATION	SECURITY REVIEW	SLA REVIEW
Tier 1— High Risk	Upon renewal or significant changes to scope of existing contract	Annually or following a security incident or breach; or significant changes to scope of existing contract	Annually or following a security incident or breach; or significant changes to scope of existing contract	Annually or following a security incident or breach; or significant changes to scope of existing contract
Tier 2— Medium Risk	Upon renewal	Every 24 months or following a security incident or breach; or significant changes to scope of existing contract	Every 24 months or following a security incident or breach; or significant changes to scope of existing contract	Every 24 months or following a security incident or breach; or significant changes to scope of existing contract
Tier 3— Low Risk	Upon renewal	Every 36 months or following a security incident or breach; or significant changes to scope of existing contract	Following a security incident or breach; or significant changes to scope of existing contract	Following a security incident or breach; or significant changes to scope of existing contract

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

03

STEP 3:

Leverage objective data and analytics to prioritize remediation efforts

Utilize data-driven insights to prioritize remediation efforts based on risk severity, likelihood, and potential impact.

In addition to what you can request from a vendor, you need objective evidence and data to validate their responses and make better decisions. Security ratings provide a wide range of insights on vendors' security controls that add another layer of verification to your vendor risk assessments, complementing security artifacts and questionnaires with objective findings on categories such as encryption, data retention, pentesting, and privacy protocols.

These findings not only trigger remediation requests, but may also give the vendor an opportunity to improve their security posture, ultimately fostering confidence across the supply chain.

Qualitative and quantitative security performance ratings, like those provided by Bitsight, have been proven to directly correlate to the likelihood of data breach at a given organization. The lower the rating, the more concerned you need to be about your data in the hands of a third party.

Bitsight metrics have the highest correlation to breaches and security incidents.

Marsh McLennan found statistically significant correlation between 14 Bitsight analytics and cybersecurity incidents.

Read the Report →

One more way to enrich the results of your risk assessments is by leveraging integrations. For instance, Bitsight VRM can integrate your automated workflow with several data feeds to gain additional intelligence on vendors, including geopolitical risk, credential exposure, privacy posture, and financial viability. Plus, you can integrate VRM with business intelligence or GRC tools to further streamline your process and augment your findings.

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

03

STEP 4:

Track, improve, report, and communicate program wins

A key way to prove value and gain both executive support and budget is to quantify and visualize cyber risk in financial terms. Demonstrate that your Third-Party Risk Management or Supply Chain Cybersecurity program creates an overall reduction in risk, and reduces or mitigates unexpected costs associated with a cyber incident, aligned to the annual loss expectancy (ALE). By measuring cyber risk in this way it is often easier to gain support and budget, especially if the cost of your program itself is less than the forecasted annual loss expectancy.

You can, for instance, calculate an annual loss expectancy from a third-party data breach by multiplying the likelihood of such a breach materializing in the next year by the financial impact of such a breach to your organization should it occur (e.g., public relations costs, disruption to your operations, legal costs, etc.). And when there is a security breach at a third-party that was rejected based upon findings from your risk assessment process, share this information with your executive team.

If you encounter roadblocks to gain or retain executive buy-in, try the following perspectives:

COMMON PUSHBACK	COMPELLING ARGUMENT
— Lack of budget dedicated to TPRM	+ Reduction of annual loss expectancy is greater than the cost of the program
— TPRM is a security priority, not a business priority	+ TPRM fuels business growth by securing outsourcing, ensuring regulatory compliance, and building customer trust
— Manual, slow exchanges across weeks, if not months	+ Automation and dedicated tools simplify TPRM to do more with the same resources

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Strategies to Simplify, Integrate, and Consolidate Your TPRM Workflow

03

STEP 5:

Ensure compliance across your digital supply chain

Regulations are bringing attention to cyber risk management and recognising the critical importance of cybersecurity to national security, economic stability, and the safeguarding of the digital ecosystem. In the European Union, NIS2 is putting the spotlight on accountability, meaning that entities not only need to implement robust cybersecurity measures but also demonstrate compliance, cooperate with authorities, manage their supply chain's security, and maintain transparency as appropriate. In the United States, the SEC requires companies to disclose "processes to oversee and identify cyber risks associated with its use of any third party service provider."

This means CISOs can turn protective controls and capabilities into business differentiators that enable growth and protect revenue. As executive boards and regulators become increasingly involved in risk discussions, they appreciate quantifiable metrics that communicate how your company performs—both absolutely and relative to industry benchmarks, especially as regulatory expectations vary across industries.

Build trust by sharing independent, comparable, and consistent benchmarking data—an objective analysis of your organization's cybersecurity performance based on quantitative data.

In order to stay aligned to emerging regulatory requirements, implement policies and procedures to mitigate cyber, legal, and financial risks associated with vendor relationships. By proactively addressing compliance obligations, you can safeguard your organization's reputation and avoid costly penalties, sanctions, loss of reputation, or additional audit requirements being mandated.

"

Key to success is ensuring your program is security led as opposed to compliance led. When this is aligned to measurable frameworks such as NIST, ISO27001, or SOC2 it builds executive and customer trust."

Tim Grieveson

Senior Vice President—
Global Cyber Risk Advisor, Bitsight

04

Future Proofing Supply Chain Cybersecurity and Resilience

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Future Proofing Supply Chain Cybersecurity and Resilience

04

04 Future Proofing Supply Chain Cybersecurity and Resilience

Future proofing is about making choices that secure your cybersecurity beyond here and now—from selecting the right partners to balancing short-term gains with long-term stability. It's a journey that demands innovation, planning, and choosing the right tools.

When your solution aligns with your long-term roadmap, you minimize disruption because it's a natural extension of your existing security infrastructure. This seamless integration allows for a smoother transition and minimizes downtime.

Future-proofing your TPRM program is securing your tomorrow today. So choose wisely, and invest strategically.

UNIFICATION

A unified approach to cyber risk management streamlines your efforts and saves you from the constant upheaval of change management and training. Your team should focus on mitigating cyber risk, not managing a decentralized toolkit.

SCALABILITY:

A capability that fits your long-term roadmap needs to integrate people, process, and technology, as well as adapt to changing requirements—whether it's an expanded vendor network, increased data volumes, or evolving compliance standards.

REGULATION READINESS:

You need flexible capabilities that can be mapped to evolving requirements—such as independent benchmarking to comply with the SEC cyber risk disclosure guidelines, or continuous monitoring of ICT third parties to comply with NIS2 and DORA standards.

> "Start with a vision of where you want to take your TPRM program, and then find the vendors and solutions that can get you there. Consider three key principles: Unification, scalability, and regulation readiness."

Tim Grieveson

*Senior Vice President—
Global Cyber Risk Advisor, Bitsight*

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Future Proofing Supply Chain Cybersecurity and Resilience

04

How Can Bitsight Empower Your TPRM Program and Supply Chain Cybersecurity?

Bitsight has been at the forefront of making cyber risk management easier and helping TPRM program managers scale their work. We pioneered the use of security ratings to measure organizations' security postures and those of their third-party vendors, integrating cybersecurity analytics with their workflows and platforms of choice.

Bitsight Third-Party Risk Management is an end-to-end solution that makes the process more efficient, helping organizations assess, validate, and continuously monitor vendor security performance with confidence. Our customers gain efficiency by executing all TPRM workflows in one platform.

Whether you're just getting started or taking your program to the next level, Bitsight has the tools and services to help your team execute on your third-party risk management programs.

Bitsight Third-Party Risk Management

Powered by Managed Services

- Managed vendor assessments
- Continuous monitoring & risk hunting
- Surfaced insights and reporting
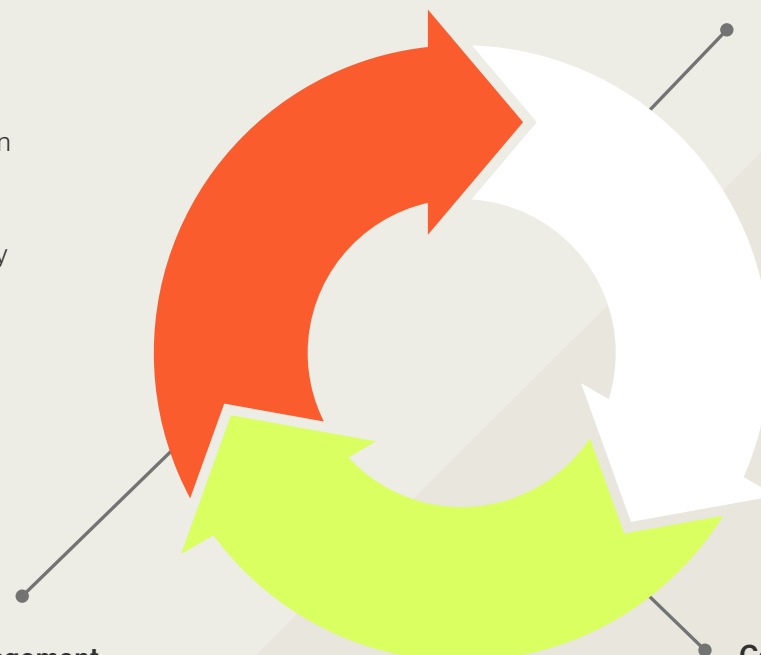
Vendor Risk Management

- Automated assessments
- Growing vendor network
- Evidence to validate

Continuous Monitoring

- Inspect vendor controls at any moment
- In-context vendor collaboration
- Automatic discovery of concentrated fourth-party risk

Exposure Management

- Accelerate vulnerability remediation
- Scale and track vendor outreach efforts
- Prioritize mitigation to exposure

5 Proven Strategies to Maximize Supply Chain Cyber Risk Management: Future Proofing Supply Chain Cybersecurity and Resilience

04

The Power of the Network

Bitsight Vendor Risk Management enables you to instantly tap into a rapidly expanding network of over 40,000 vendor profiles—continuously updated—all in real time. The efficiency gains are extraordinary. The experience is even better.

40K+
Vendor profiles

3X ROI
Within first
six months*

90%
Vendor
acceptance rate*

75+%
Time reduction
assessing
vendors*

*As reported by existing Bitsight customers. Actual outcomes will depend upon a variety of factors unique to each customer and are not guaranteed.

Request a personalized demo today and start building your integrated TPRM program.

Get started today →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ)   RALEIGH   NEW YORK   LISBON   SINGAPORE

BITSIGHT