AI-powered third-party risk management playbook

Optro

Table of contents

Introduction

Many organizations are ramping up their third-party risk management (TPRM) efforts due to a number of high-profile third-party security breaches that have peppered recent headlines. As the reputational, operational, and financial fallout from these security incidents proliferate, organizations cannot afford to overlook or deprioritize third-party vendor risk, especially in an increasingly interdependent global business environment. Verizon's 2024 Data Breach Investigation Report — which studied over 10,000 incidents — found a **68% increase in breaches involving a third party between 2023 and 2024.** In these breaches where there was a supply chain connection, the incident occurred because either a business vendor was the vector of entry for the breach, the data compromise happened in a third-party data processor or custodian site, or the breach involved a third-party security breach.

An August 2024 Optro flash poll of **over 830 cybersecurity professionals found over 90% of respondents experienced at least one IT incident a year caused by a third party.** Moreover, **36%** of respondents experienced a third-party related security incident **once per quarter**, while **11%** experienced an incident **once per month.**

IBM found the global average cost of a data breach averaged $4.8 million in 2024 — a 10% increase over last year and **the highest total ever**. Furthermore, a report by Gartner Research found the cost of a **third-party cyber breach** is typically **40% higher** than the cost to remediate an internal cybersecurity breach.

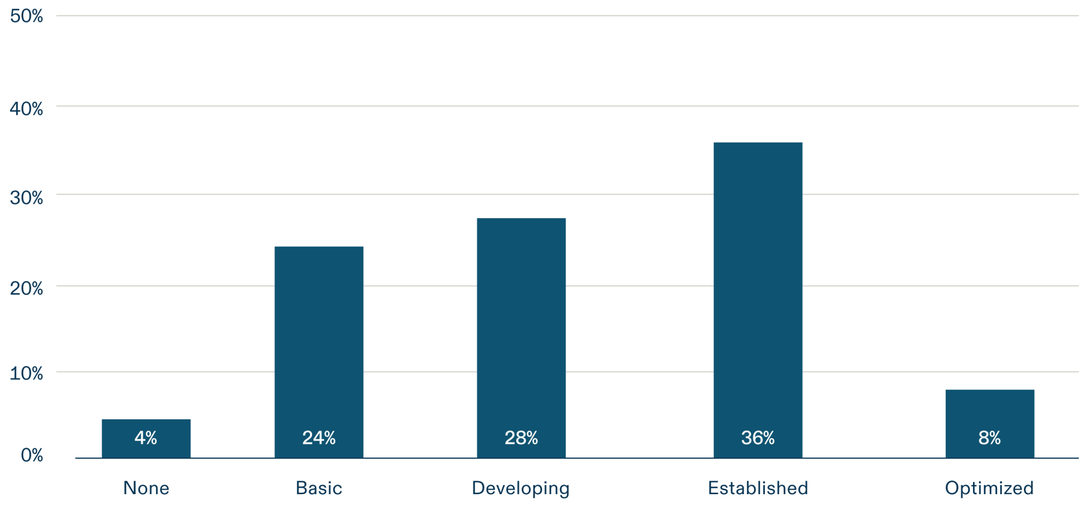
These statistics all point to the need for organizations to prioritize strong TPRM practices in their overall risk management efforts. Many organizations, however, are still struggling to get TPRM right. A July 2024 survey of security and IT leaders by Optro and CyberRisk Alliance found about 44% indicated their organization has an “Established” or “Optimized” third-party cybersecurity risk management program. Meanwhile, 24% of those surveyed have a Basic program (mostly ad-hoc/reactive with some techniques inconsistently applied) and 28% have a Developing program (framework developed, processes partially implemented).

How would you rate your organization’s TPRM program maturity? Do your policies and processes provide adequate protection against critical third-party risks — or are you doing the bare minimum to identify and track some third-party partners? With businesses today more connected and interdependent than ever before, any third party can present risk to your organization at any time. This includes not only **vendors and suppliers but also partners, customers, and third-party software providers**.

While the risk has never been higher, the good news is that the processes and technologies supporting effective TPRM have greatly improved in recent years. With so much at stake, there is no better time than the present to level up your third-party risk management strategy. This ebook includes key TPRM principles and tactics designed to help you mature your organization’s third-party risk practices. No matter where you are on the TPRM maturity scale, taking advantage of this guide’s best practices and technology tips can help you move the needle forward in effectively managing third-party risks.

Organizations must prioritize strong TPRM practices in their overall risk management efforts.

Only 8% of organizations have optimized their TPRM program, which is a massive risk exposure.



Source: Optro and CRA, From trust to security: Third-party risk management strategies and challenges

Did you know?

The Institute of Internal Auditors (IIA) released the TPRM Topical Requirement as part of their 2024 update to the Standards, signaling a heightened emphasis on third-party risk oversight. The TPRM Topical Requirement provides specific guidance, including a standardized framework, for internal auditors on assessing the design and implementation of third-party governance, risk management, and control processes.

What does this mean for you? Adopting this framework offers a valuable opportunity for your organization to standardize and streamline its TPRM program, ensuring consistent, compliant risk management practices across the board. Now is a great time to review the draft guidance here and reach out to your audit colleagues to collaborate on and streamline your compliance efforts.

Third-party risk management programs: Overview

Guiding principles

A TPRM program provides discipline, structure, and oversight to guide the plans, policies, and processes by which your organization:

Identifies and categorizes the third parties you engage. You can't manage risk effectively without a regularly updated inventory of all potential sources.

Understands and prioritizes the risks presented by third parties. Not all third parties present equal risk and should not consume equal risk management capacity.

Establishes and enforces key controls for mitigating those risks. Third-party risk/controls assessments should address and prioritize the risks that matter most to your organization. Set up contracts, expectations, and service-level agreements (SLAs) to hold third parties accountable for effectively managing those risks.

Performs monitoring that tracks and regularly reassesses third-party relationships and risk exposures. Risk is dynamic, changing over time. Design TPRM policies and processes to help you catch and respond to the changes that matter.

Responds to real-time issues and communicates TPRM awareness and accountability throughout the organization. Everyone can play a role in managing third-party risk. TPRM policies, protocols, and reporting should support organization-wide awareness of key risks, ongoing engagement with third-party relationship owners, proactive TPRM practices, informed decision-making, and timely, effective issue responses.

Common program components and qualities

TPRM programs vary based on the size, scope, resource and budget constraints, regulatory requirements, and risk profiles of the organizations for which they're built. One size does not fit all — but all programs are made of several general components:

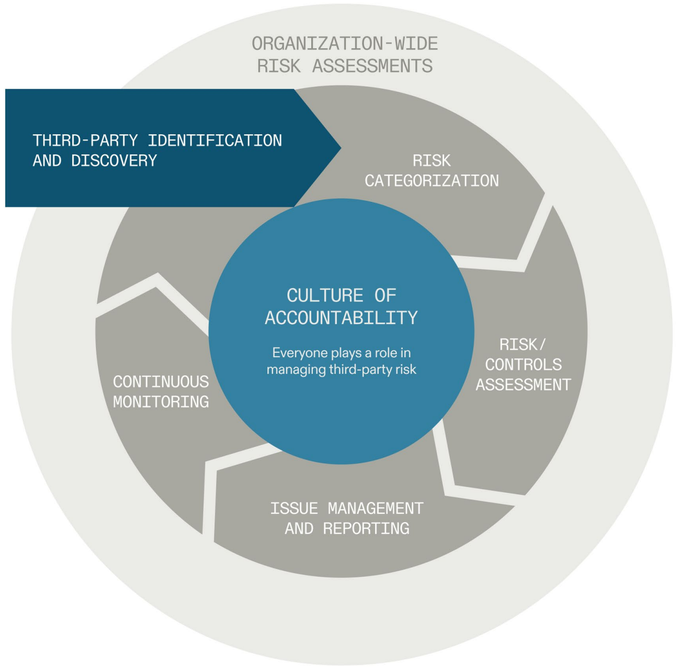
1. Planning and Onboarding
2. Due Diligence
3. Contracting
4. Ongoing Management
5. Periodic Reassessment
6. Offboarding

In addition, as depicted in the overview graphic, TPRM programs:

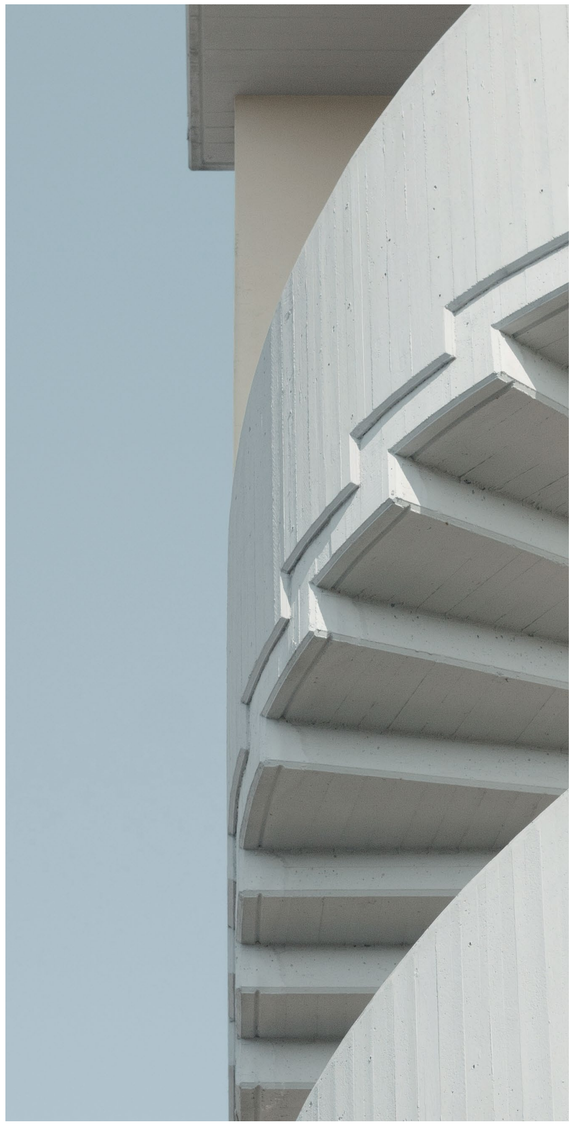
- **Are continuous.** As new third parties enter the equation and existing relationships evolve over time, you should periodically revisit risk categorization, assessment, issue management, reporting, and continuous monitoring.
- **Occur against the backdrop of your organization's enterprise and cyber risk assessment(s).** As your risk profile, exposures, and prioritization evolve, so must your TPRM program's focus and goals.
- **Are best built around a culture of accountability.** TPRM responsibilities are often distributed across a range of functions and business units. Set the tone that everyone has an important role to play in managing the risks presented by the third parties they engage with.

Culture plays a huge role in the success of your TPRM program.

A connected approach ensures that everyone plays a role in managing third-party risks.



Common gaps and obstacles

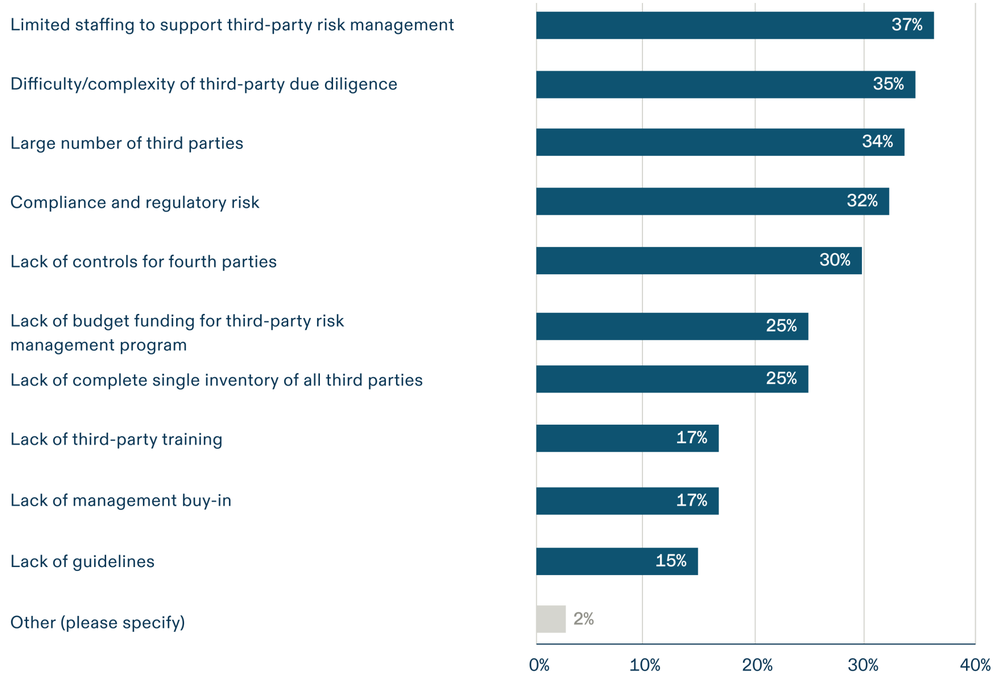


All organizations face challenges in establishing effective TPRM programs. A research report by Optro and CyberRisk Alliance found that limited staffing to support third-party risk management was the most commonly cited challenge, while difficulty/complexity of third-party due diligence, and a large number of third parties, followed closely behind.

Whatever your biggest challenges, improving your understanding of key TPRM tactics and success factors can help you close gaps and overcome obstacles.

Complexity is one of the top challenges organizations face when managing third-party risk.

37% of organizations don't have the necessary resources to manage third-party risk, while 35% struggle with the complexity involved.



Source: Optro and CRA, From trust to security: Third-party risk management strategies and challenges

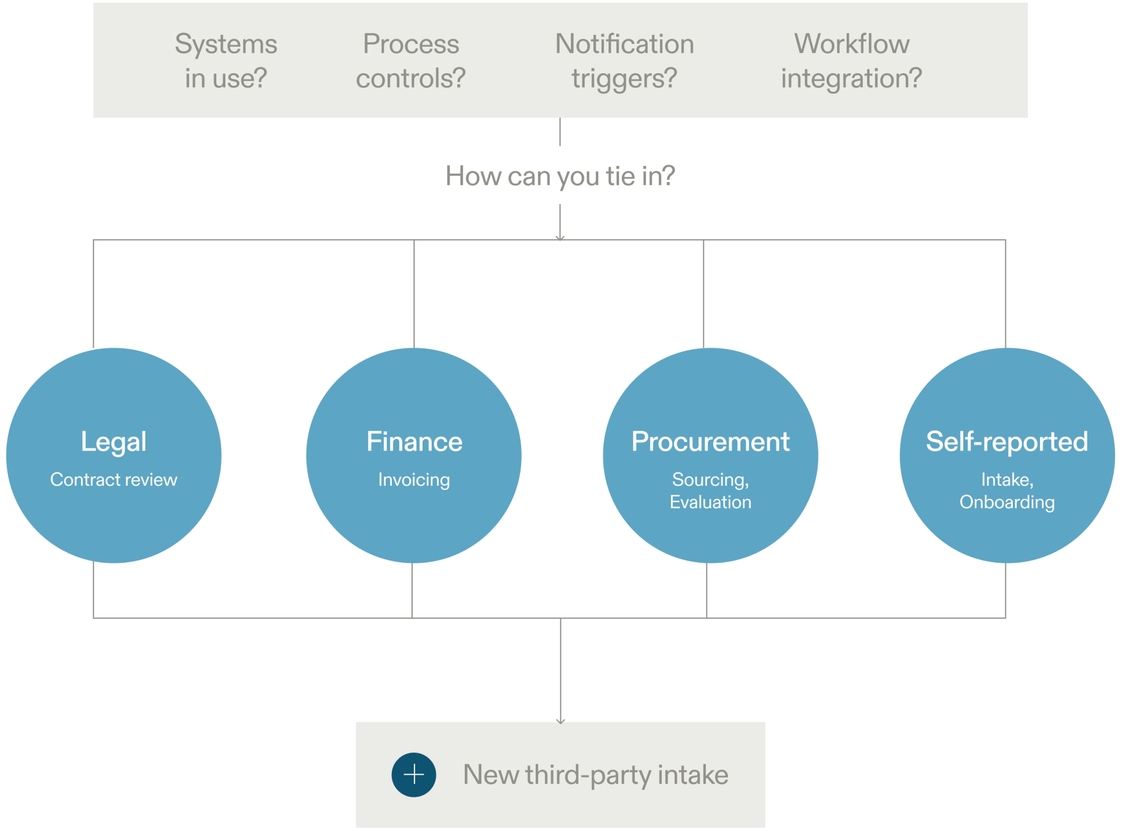
Third-party identification and discovery tactics

What's the best way to formalize your plan, policies, and processes for continually identifying the new third parties working with your organization?

Ensure ongoing visibility between the “where” and the “who”

The most important tactic is to:

1. Assess *where* in your organization new third-party engagements are initiated.
2. Identify *who* is responsible for assessing and making decisions about relationship risk.
3. Build a process that ensures ongoing visibility between the *where* and the *who*.



Enable smart and proactive resource deployment

Create and promote clear, readily available TPRM policy and process guidance.

Use simple vendor request and review forms at the point of intake.

Establish a complete, regularly updated inventory of third parties.

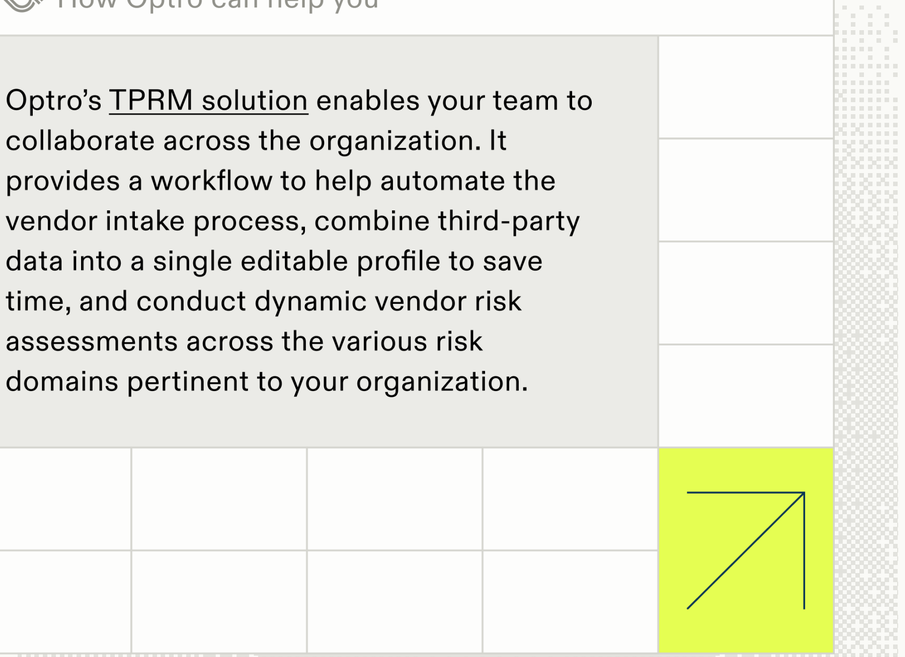
Scale assessment and remediation approach(es) as appropriate to match risk levels.

Ensure that vendors' technology and controls align with internal policy requirements, like AI governance policies for example.

Consider technology tools that create a safety net and enable ongoing visibility. For example, automated discovery tools that connect to payment or contracting systems (e.g., G2 Track) can be set up to provide alerts following triggers you establish.

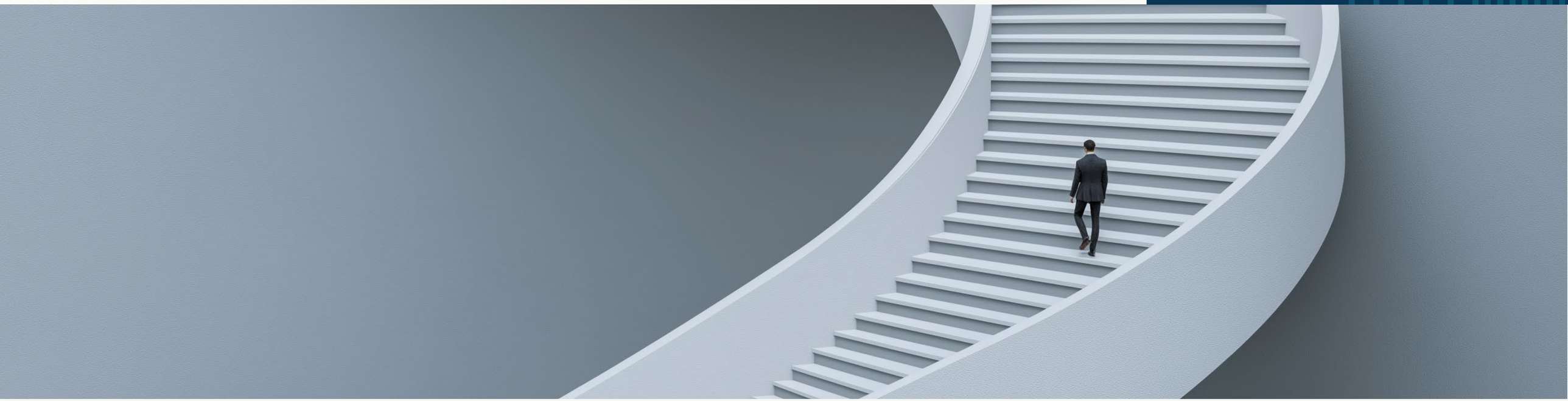
How Optro can help you

Optro's TPRM solution enables your team to collaborate across the organization. It provides a workflow to help automate the vendor intake process, combine third-party data into a single editable profile to save time, and conduct dynamic vendor risk assessments across the various risk domains pertinent to your organization.



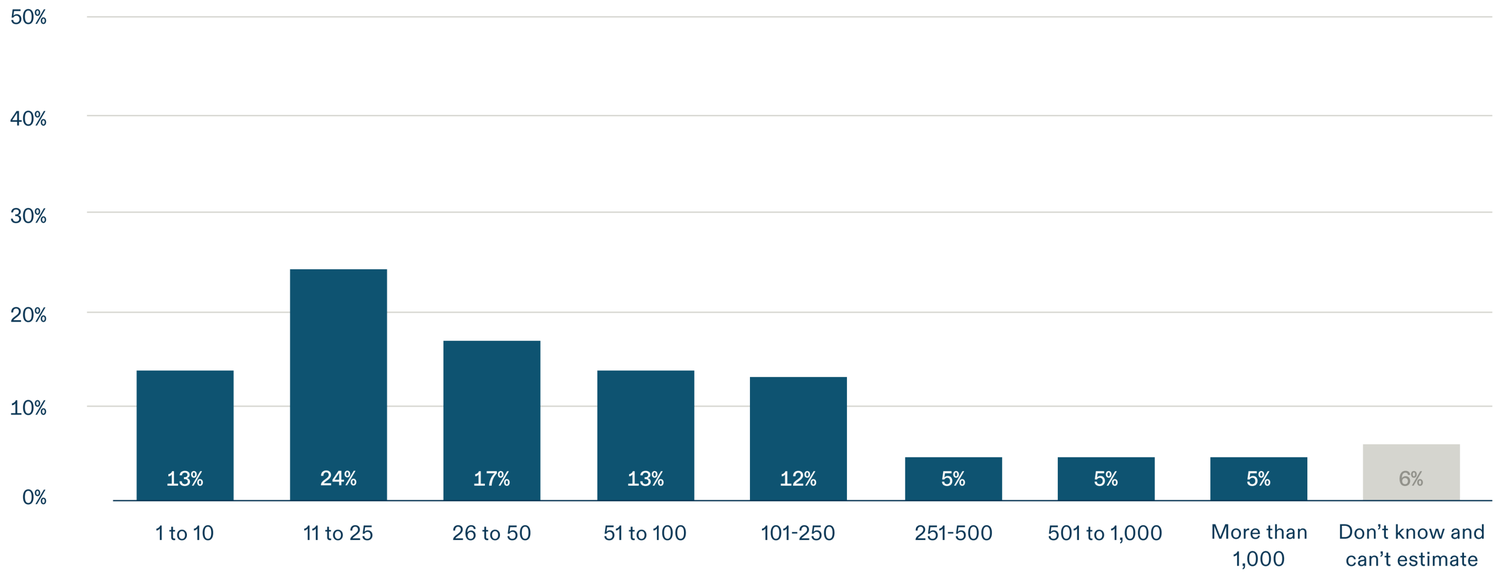
Third-party risk categorization tactics

A recent research report conducted by Optro and CyberRisk Alliance found that 40% of infosec professionals surveyed reported that their company is working with more than 50 third-party contractors, and 15% said that their company is working with more than 250 outside partners. Whether your organization works with 10, 1,000, or 10,000 third parties, the problem is the same: You have finite resources. How can you deploy them most effectively?

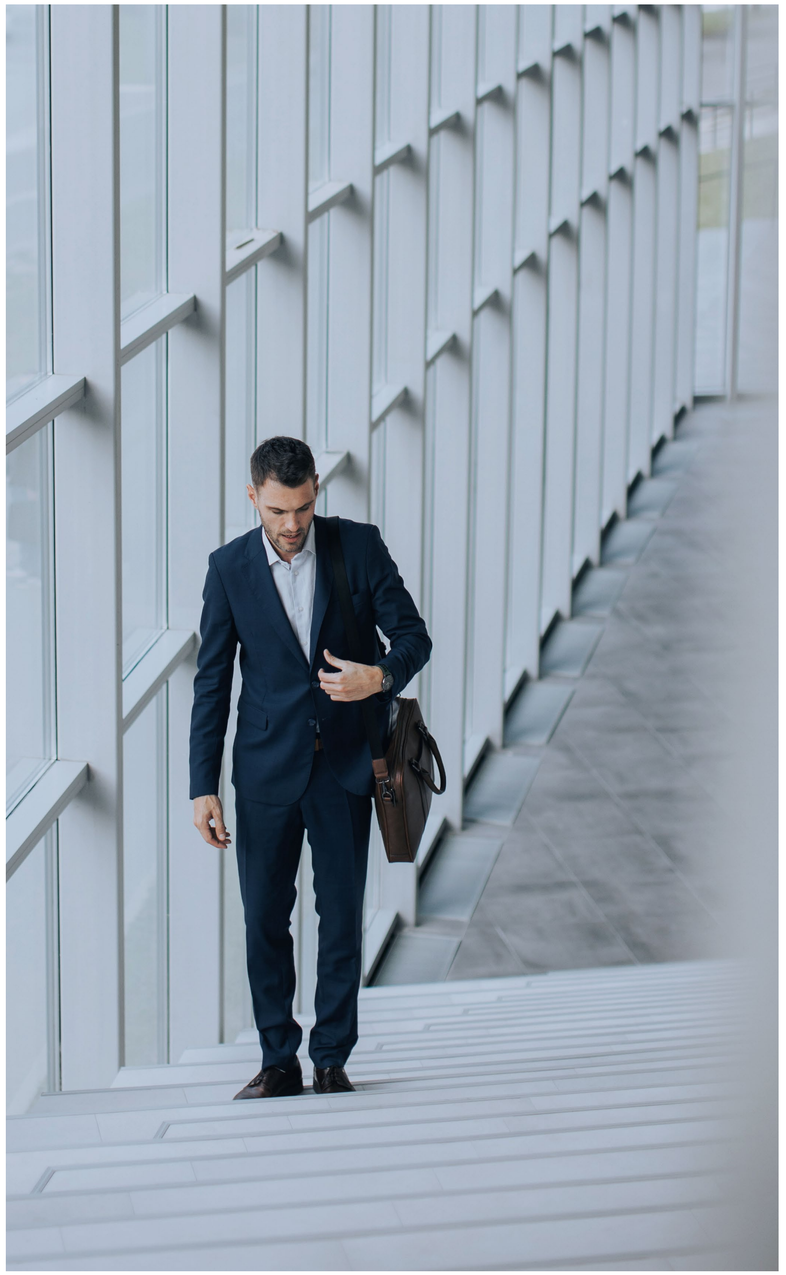


Organizations are working with more third parties than ever.

40% of infosec professionals surveyed reported that their company is working with more than 50 third-party contractors.



Source: CyberRisk Alliance Business Intelligence (CRA BI), Third-Party Risk Survey, June 2024.



Stratify third parties in proportion to risk level

Since all third parties do not present equal risk, they should not consume equal risk assessment capacity. Develop criteria to help you categorize third parties into high-, medium-, and low-risk buckets that help you better allocate your limited resources where they'll have the most impact. Creating and updating third-party risk categorization is a key success factor for any TPRM program.

Begin by referring back to your enterprise and cybersecurity risk assessments, assessing each third party based on the risks that matter most to your organization. For example, if access to confidential data is the most important consideration for your organization, you may establish the risk tier categories shown in the table.

Based on the risk profile of your organization, you could also consider categorizing third parties based on questions such as:

- Is the third party a critical dependency to meet organizational objectives?
- Will the third party have access to confidential or customer data?
- Will the third party directly access your infrastructure, networks, or systems?
- Does the third party support the availability of customer-facing services?
- Does the third party support any critical internal business functions?
- Can the third party impact your organization's reputation or business relationships?
- What is the estimated spend?
- How many internal users, teams, functions, or processes will rely on this third party to perform?

Risk categorization example

RISK TIER CATEGORIZATION	TIER 1 HIGH RISK	TIER 2 MEDIUM RISK	TIER 3 LOW RISK
Data Access	Confidential	Proprietary	Public or None
Review Frequency	1 Year	2 Years	3 Years
Review Requirements	Onsite Audit Controls Questionnaire Certification Review	Certification Review	None

Ensure realistic, appropriate distribution across tiers

Keep an eye on distribution across tiers. Most third parties should fit into Tiers 2 and 3. Be very discerning with categorizing third parties as Tier 1, since that's where you'll invest the most time and resources.

How Optro can help you

Optro's TPRM solution enables your teams to categorize vendors based on criticality during the intake process and a workflow to periodically reassess these vendor risk categorizations. By standardizing this across your organization, you can better allocate teams' time to high-risk vendors. Workflows can also be automated based on these vendor categories, saving time and making sure your highest-risk vendors are always being assessed on a timely basis.

Risk/controls assessment tactics

What tactics can you use to better understand and mitigate third-party risks and controls? TPRM programs commonly employ a range of tactics.

The most important success factor is ensuring tactics are proportional to the level of risk each third party presents to your organization.

Security controls questionnaires

The most common tactic is the security controls questionnaire. This extremely flexible approach allows you to customize each questionnaire based on the type of third party and the risks you are concerned with. Since you can be highly detailed and prescriptive about the controls you expect to be in place, this approach can provide confidence that third parties are appropriately controlling the risks you care about most.

PROS

Customizable based on:

- Vendor type
- Use cases
- Data classification
- Level of access
- Likely risk/impact area

CONS

- Highly manual
- Subjective
- Time-consuming (for both your organization to create, and third party to respond to)

SAMPLE USE CASE

Third party will have access to proprietary data. You tailor the questionnaire to detail the exact numbers and types of data security controls required.

Standardized questionnaires

Another common tactic is standardized questionnaires. Standardized questionnaires have been developed through the collective knowledge and experience of a range of security experts and technology organizations. Widely used options include Shared Assessments' Standardized Information Gathering Questionnaire (SIG) and Cloud Security Alliance's Cloud Control Matrix (CCM) Consensus Assessment Initiative Questionnaire (CAIQ). Third parties may be familiar with and have ready responses to these questionnaires.

PROS

- Standardization, with some customization options
- Easy to compare responses from different third parties
- Faster turnaround time

CONS

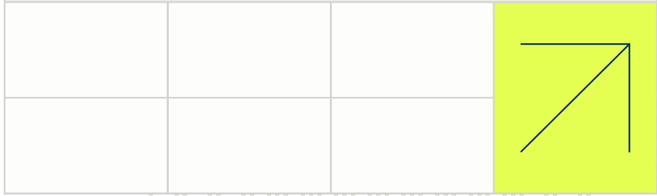
- Highly manual
- Subjective
- Time-consuming

SAMPLE USE CASE

Your RFP requires third parties to complete SIG as part of initial vetting so you can screen out and make apples-to-apples comparisons.

How Optro can help you

Optro's TPRM solution offers teams the option of leveraging either security control questionnaires or standardized questionnaires with our Automated Assessment Completion feature. Powered by Optro AI, Automated Assessment Completion leverages a document provided by the vendor, such as a SOC 2 report, and suggests the correct answers to the questionnaire based on the analyzed document. This greatly reduces the time it takes for vendors to complete these questionnaires while still providing organizations the flexibility to assess risk within their security context.



Compliance certifications and reports

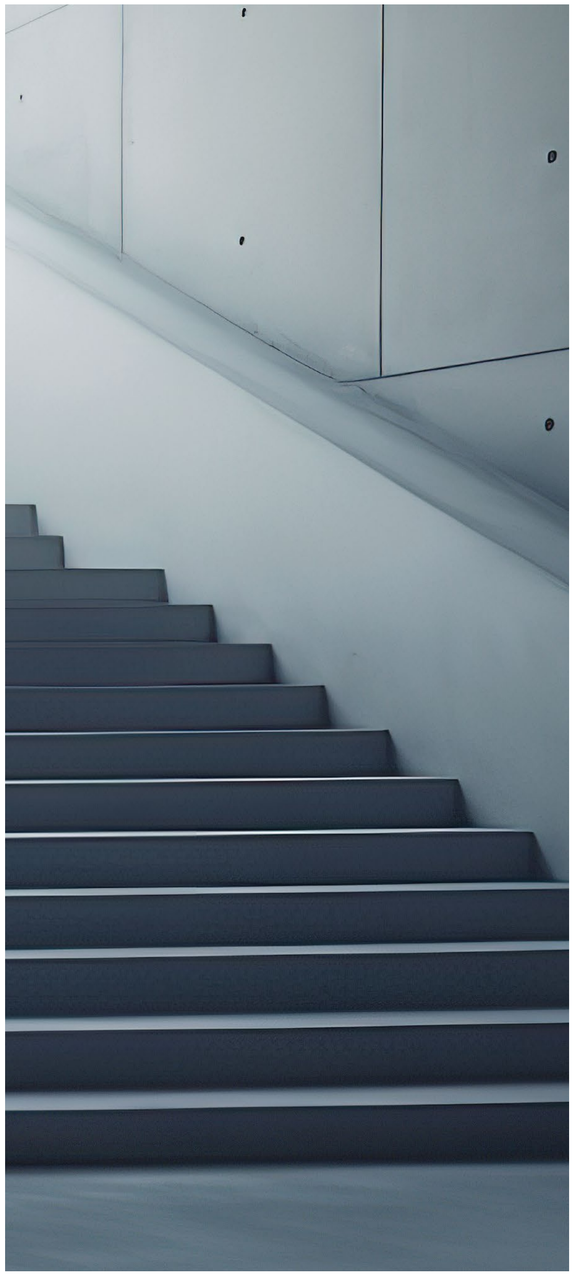
Security frameworks are blueprints for security programs that effectively reduce and manage risk. For lower-risk third parties, you may be able to gain appropriate assurance by reviewing and confirming any regulatory or security-focused certifications and reports they have earned.

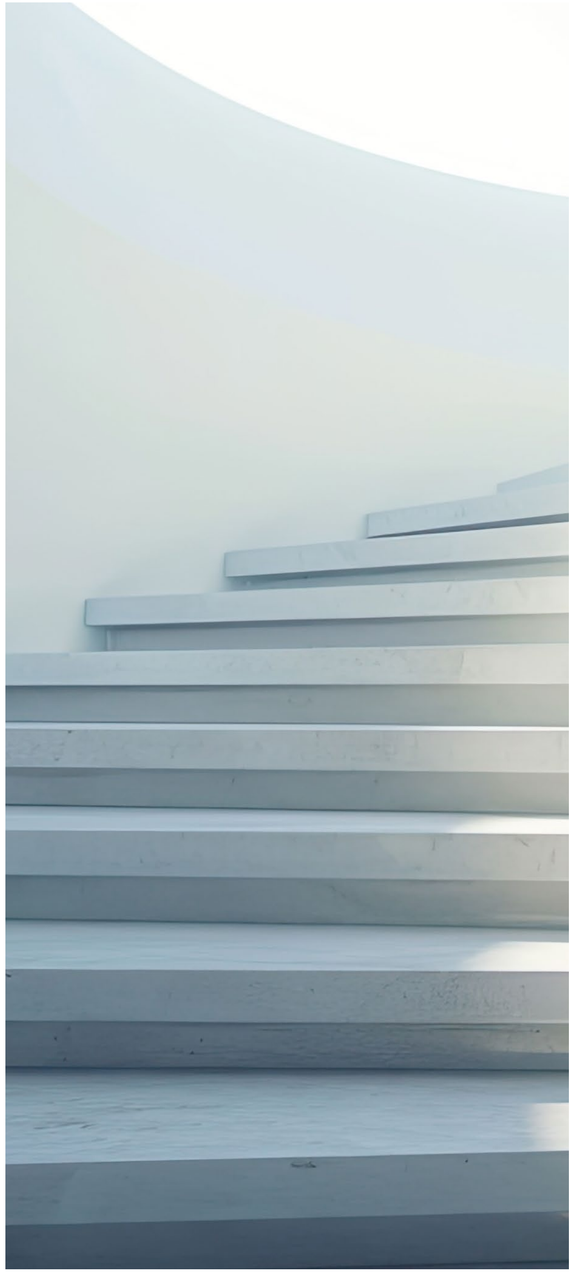
PROS	CONS	SAMPLE USE CASE
• Regulatory requirements met • Third-party-verified (not subjective) • Cost-effective • Time-effective, expediting review process	• Could lack specificity or applicability to the risks you're most concerned about	Your primary concern is whether the vendor is suitable for handling regulated data, such as credit card information. You require a PCI Certification to prove that the vendor is suitable and has been reviewed by a third party.

Onsite audits

Onsite audits allow you to take a fully customized first-hand look at how third parties address the risks you care about. You (or your third-party risk assessment provider) can directly verify and evaluate their internal policies against risk. But while onsite audits are the safest and most effective way to assess third-party risk, they are neither cost- nor time-effective. They should generally be reserved only for your highest-risk third parties — those presenting critical risks to your organization.

PROS	CONS	SAMPLE USE CASE
Ability to: • Interview key control owners • Validate control testing • Collect evidence	• Very costly • Very time-consuming • Tough to negotiate in a third-party contract	A third party is deeply ingrained in your processes and networks, presenting an existential level of risk to your organization. You contractually require permission for onsite audits.





Contract reviews

Contract reviews can be an effective way to invest resources in evaluating third-party risk and controls. While contract reviews are generally performed by your legal team, it's ideal to include your risk team in the process. You can also embed language that helps you gain a higher level of assurance that third parties can be held accountable for meeting control obligations.

PROS	CONS	SAMPLE USE CASE
• Higher level of assurance • Legally actionable • Ability to embed specific requirements for controls or gap remediation	• High-effort • Tedious and time-consuming to review • Negotiation reluctance from third parties	You uncover gaps in a third party's security framework. Instead of calling off the deal, you embed a clause requiring them to remediate gaps to a certain level by a set date.

Reputation services

Third-party reputation services are a relatively recent evolution. By crowdsourcing risk assessments (CyberGRX) or scraping websites, DNS and TLS configurations, and other publicly available data for objective, verifiable security information (BitSight), these services develop third-party risk ratings — essentially "security credit scores."

How Optro can help you

Optro's Third-Party Risk Management solution integrates SecurityScorecard ratings data directly within the context of third-party vendors, enabling teams to evaluate and manage risk collaboratively with their vendors. SecurityScorecard monitors the threat landscape, scanning billions of signals each week to help you identify hidden risks so you can take action. With this integration, teams can stay ahead of vendor risk monitoring and manage their mitigation plans more effectively and accurately.

Sample reputation service reports

PROS	CONS	SAMPLE USE CASE
• Low effort for your organization • Third-party-verified (not subjective) • Easy to share reports with partners	• Could lack specificity or applicability to the risks you're most concerned about • May use only existing publicly available info	You lack TPRM resources. To save time and effort in assessing lower-risk third parties, you use a reputation service to access risk reports.

Timely monitoring tactics

Given your organization's risk prioritization and TPRM categorizations, how should you tailor monitoring tactics to match?

Establish periodic reassessment cadence based on risk level

Again, the most important success factor is to structure and formalize continuous monitoring activities based on risk level. Higher-risk third parties should receive more attention more frequently, and lower-risk third parties should receive less attention less frequently.

Periodic reassessment cadence example

RISK TIER	CONTRACT REVIEW	RISK CATEGORIZATION	SECURITY REVIEW	SLA REVIEW
Tier 1 — High risk	Upon renewal	Annually	Annually	Annually
Tier 2 — Medium risk	Upon renewal	Every 24 months	Every 24 months	Every 24 months
Tier 3 — Low risk	Upon renewal	Every 36 months	Not required	Not required

Perform rediscovery with internal relationship owners

Risk changes over time, so reassessments should involve appropriate rediscovery with your organization's third-party relationship owners. This will help ensure that TPRM approaches and categorization remain appropriate for each third party.

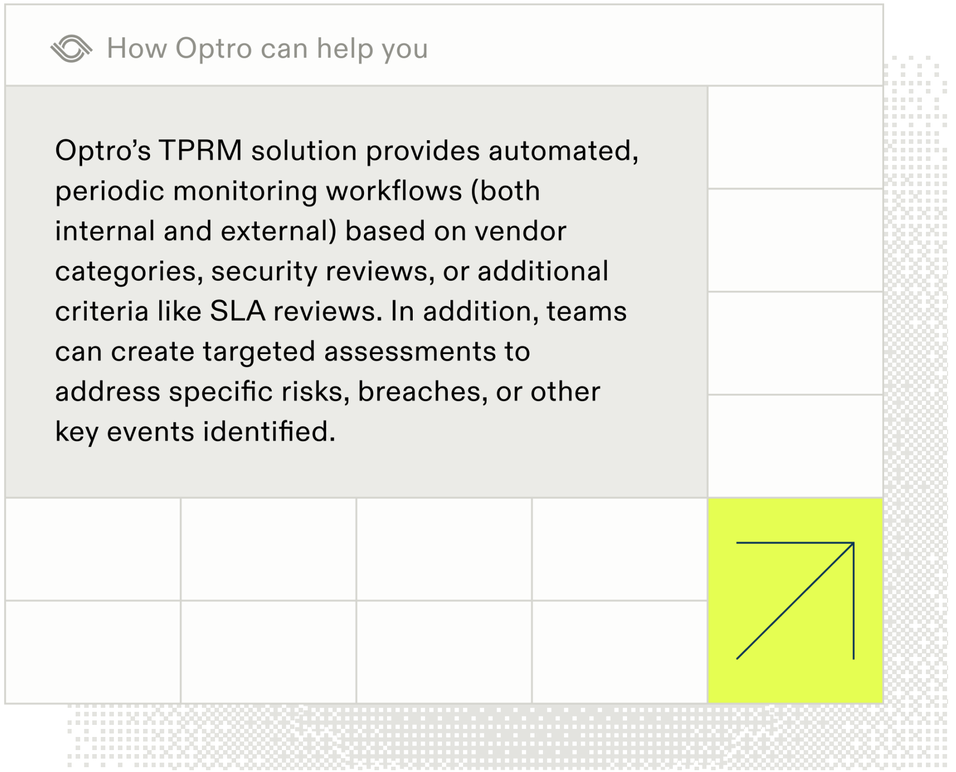
Most often, rediscovery occurs via surveys that are either sent manually or triggered within an automated technology platform. Surveys should address:

- **Relationship ownership.** Are they still the owner?
- **Risk categorization.** Have the use cases that the third party is addressing changed? Have there been changes to the third party's risk profile?
- **Contract renewals.** Should terms be restructured to better manage risk or account for new considerations?
- **SLAs.** How do they feel about the third party's overall performance? Are SLAs being met? While SLA review isn't typically part of the risk mandate, reassessment touchpoints are a great opportunity to assess SLA compliance.

Perform targeted assessments following key events

You may want to re-engage third parties outside your normal cadence to either re-assess or perform a targeted assessment:

- After a security incident or breach.
- After a public zero-day, if it's likely the third party was impacted.
- After you've updated your internal risk assessment(s).



Issue management and reporting tactics

How can you ensure that your TPRM program drives optimum value for your business?

Focus on meaningful, effective reporting

The key success factor is creating meaningful reporting that regularly communicates risk information and insight to the right people across your organization. As depicted in the graphic, effective TPRM issue management and reporting are symbiotic, benefiting and supporting each other in turn. Meaningful reporting helps to create ongoing awareness of key gaps and risks. When awareness is raised with the right people, reporting remains meaningful and accurate. People are equipped not only to avoid issues but to respond more effectively when they occur.

Build accountability around regularly updated risk assessments

Just as in the overview graphic on page 6, effective TPRM programs occur against the backdrop of regularly updated organization-wide risk assessment(s) and around an overall culture of accountability. The risks stemming from control gaps or other identified issues with third parties should be quantified and rolled up from the relationship owner to the executives responsible for owning the overall risks for their area of the organization. As a result, relationship owners can collaborate with risk owners on the tradeoffs of engaging this third party, changing how they negotiate that third party's contract and SLAs, implementing compensating internal controls, or causing them to engage a different third party altogether.

Create reporting that supports effective decision-making

Ensure that your TPRM reporting format and cadence are designed to help executive leadership and relationship owners understand and use risk data to better manage and mitigate third-party risk. Reporting should help people readily understand which third parties present the most risk to the business, which areas of the business are most affected by third-party risk, and the plans to mitigate those risks.

Conclusion

Many of the organizations impacted by third-party risk incidents over the past few years are still in damage control mode. Their valuable risk resources remain focused on responding to past incidents rather than proactively preventing future occurrences.

These organizations are still vulnerable. Will they survive the next third-party impact?

Against an ever-evolving risk landscape in which third parties present significant risk, businesses can no longer afford to treat TPRM as a low-priority, check-the-box exercise. Fortunately, the majority seem to have learned this lesson. A 2024 research poll conducted by Optro and CyberRisk Alliance found about half of all respondents surveyed indicate that third-party risk is either **a high priority or critical priority** at their organization.

Remember, TPRM is primarily about making strategic use of limited resources. Is your risk team focused on the third parties and risks that have the most potential impact? Which tactics will help you be more proactive in managing third-party risk? Are there opportunities to more effectively use existing or new technologies (e.g., information security and risk management software) for third-party discovery, monitoring, and reporting activities? How can you optimize your TPRM program to make better decisions for your business?

If your organization hasn't yet prioritized its TPRM program, the time to act is now. Don't let your organization become the next third-party security breach headline.

About the authors

Richard Marcus

Richard Marcus, CISA, CRISC, CISM, TPECS, is the CISO at Optro, where he is focused on product, infrastructure, and corporate IT security, as well as leading the charge on Optro's own internal compliance initiatives. In this capacity, he has become an Optro product power user, leveraging the platform's robust feature set to satisfy compliance, risk assessment, and audit use cases. Connect with Richard on LinkedIn.

John Duffield

John Duffield is a Manager of Product Solutions at Optro. In his role, he meets with prospective customers to understand their functional processes and identifies how Optro can help support their risk functions and solve current state challenges. John sits on the product council as the Solutions Engineer Lead for the Third-Party Risk Management (TPRM) product and facilitates the discussion of customer feedback used to prioritize the product roadmap and future development in support of customers' requirements. Prior to Optro, he was a risk advisory consultant at EY where he focused on third-party risk and IT assurance.

About Optro

Optro's mission is to be the category-defining global platform for connected risk, elevating our customers through innovation. More than 50% of the Fortune 500 trust Optro to transform their audit, risk, and compliance management. Optro is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte.