MITRATECH
Prevalent

## Measuring What Matters:

# How to Build Effective Third-Party Risk Metrics

# Table of Contents



As organizations become increasingly interconnected, granting third parties access to data and systems becomes not just beneficial, but necessary. This, however, can open the door to third-party vulnerabilities and incidents like data breaches and supply chain attacks, with the potential for severe consequences. Boards of directors and business leaders are thus demanding more visibility across their organizations' vast third-party ecosystems.

To mitigate the impact of these risks, it is crucial to understand this multifaceted ecosystem and its moving parts: the people, processes, and technology involved. **Third-party risk management** (TPRM) can help you tackle these challenges. When implemented correctly, a TPRM program enables you to identify and mitigate risks before they can negatively impact your organization.

## TPRM Reporting: A Complex Task

While TPRM reporting is critical for identifying and prioritizing risks, it can be a complex endeavor for nascent and experienced teams alike. Even identifying a starting point can be a complicated task. As a result, many teams struggle to effectively communicate third-party risks — and some still rely on outdated, overly technical, and complex methods and dashboards. It's no surprise that the topic of third-party risk often spurs confusion between the board, executive leadership, and functional teams.

It's therefore crucial to identify, formulate, and implement the appropriate TPRM metrics for your organization. Addressing the challenges associated with identifying and mitigating third-party risks also calls for thorough planning and a comprehensive understanding of the **correlation between metrics and business objectives**.

Determining and implementing the appropriate TPRM metrics can be daunting, so your team might be asking the following questions:

- Where should we initiate measurement?
- What types of data should we monitor?
- Which metrics are meaningful and relevant?
- How can we cohesively present the data?

## How this White Paper Will Assist You

To address these concerns, this white paper will:

- Explain what TPRM metrics are and why they're essential
- Guide you through the process of developing and implementing the right TPRM metrics across different stages of the third-party vendor risk management lifecycle
- Share best practices and critical factors to consider when formulating TPRM metrics

This paper is for teams such as Risk Management, Procurement and Sourcing, Security and IT, Audit and Compliance, Data Privacy, and others responsible for identifying and implementing TPRM metrics.

# TPRM Metrics and Their Significance

Before deciding which metrics to set up, we need to delve into what TPRM metrics are, their importance, and what types of metric categories you should be aware of.

TPRM metrics are indicators that assist an organization in gauging the progress of its TPRM strategy and program. When executed correctly, these metrics reassure the organization's leadership, board of directors, and auditors that the third parties they work with pose an acceptable level of risk. If these third parties are associated with unacceptable risks, then having the right metrics will simplify the remediation and mitigation processes.

To that end, it's important for an organization to have meaningful metrics that consist of a consolidated set of key risk indicators (KRIs) and key performance indicators (KPIs). These will aid in reducing the analysis of large, complex security dashboards and enable teams to filter the relevant data they need to identify and remediate risks.

> **The reality is that a good (TPRM) program is going to be iterative, and the metrics should reflect that in year one, which will then be supplemented by what you get in year two. You need to refine it every three, six, nine months or so, and you work towards a goal over a multi-year journey.**

Identifying, formulating, and tracking the right TPRM metrics are crucial tasks for the following reasons:

- **Vendor Performance Management:** Many organizations lack a simple way to manage service level agreements (SLAs) with their vendors, increasing the likelihood of risks being introduced into the ecosystem. Implementing tools, metrics, and programs that facilitate continuous monitoring of contractual provisions will enable you to ensure that SLAs are met.
- **Board and Stakeholder Reporting:** With the right metrics, teams can regularly update the organization's board of directors, management, and auditors, enabling them to **make informed decisions** about any potential risks that arise.
- **Continuous TPRM Program Improvement:** Measuring the right TPRM metrics not only enables teams to identify and mitigate potential risks, but also assists various departments in coordinating **third-party risk assessments** and in onboarding, managing, and offboarding third-party vendors.
- **Risk Identification and Assessment:** It's vital for teams to be able to discern and assess various levels of risk across the entire third-party vendor lifecycle. Unique metrics for onboarding, management, and offboarding will reveal relevant risks for teams to proactively address at each stage.
- **Compliance and Regulatory Requirements:** With approximately 160 different global legislations and frameworks such as ISO, CCPA, GDPR, PCI, and NIST — each with its own requirements for managing third-party risk — it's essential for organizations to appropriately govern third parties and meet compliance requirements.
- **Financial Considerations:** The introduction of TPRM metrics is also crucial to an organization's vendor selection, contract negotiation, and termination processes. These metrics enable teams to plan, monitor, identify, and mitigate any detected risks.

# Developing TPRM Metrics

Having examined the significance of TPRM metrics, let's delve into the process of developing effective TPRM metrics for teams to use. Figure 1 below illustrates the process:

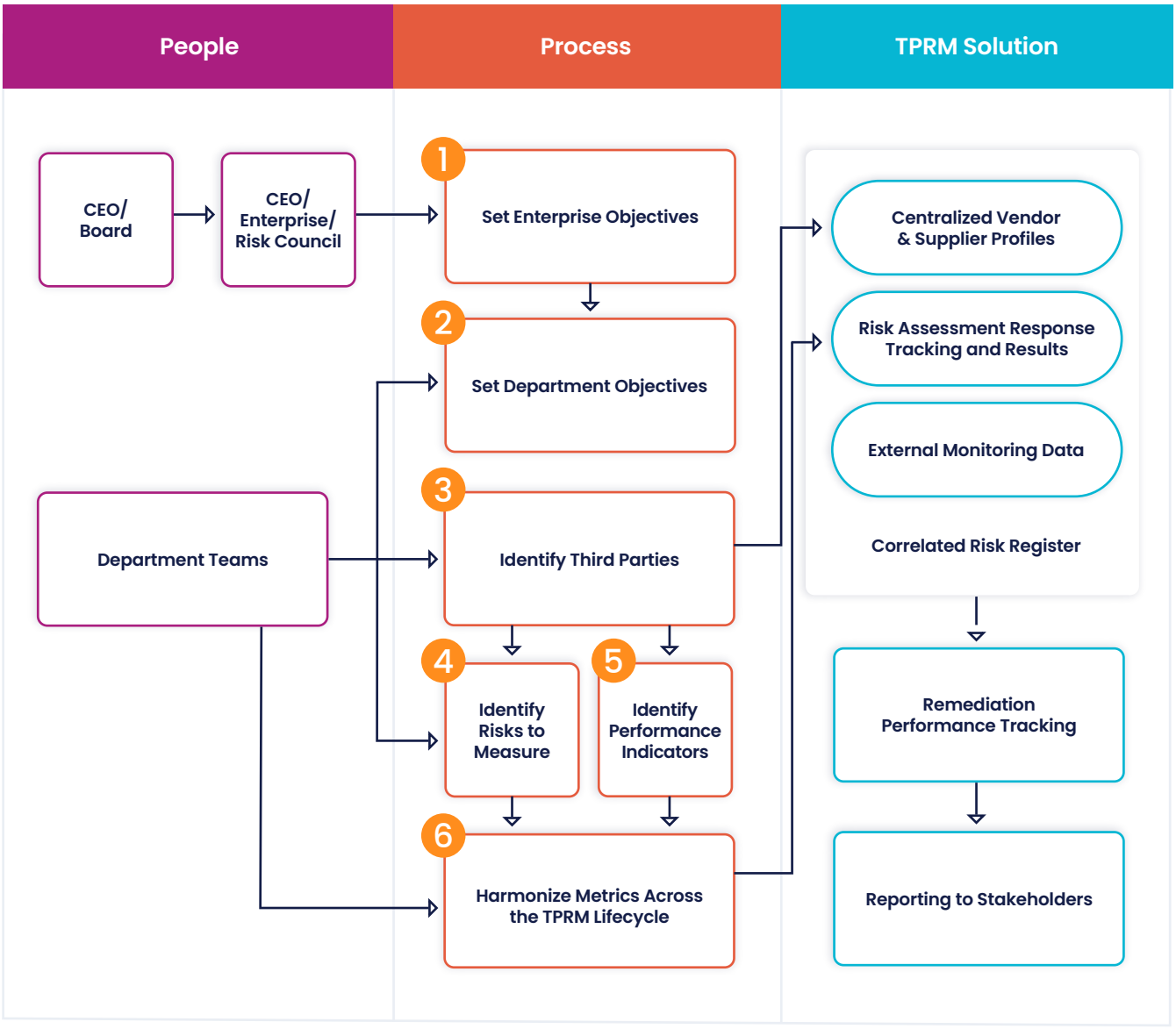


*Figure 1: The TPRM Metrics Development Process*

# People: Appointing Leadership

The organization's CEO and board of directors will often direct the chief risk officer (CRO) to orchestrate and harmonize the process through an enterprise risk council (ERC), a working group that consists of members from different business units. In the case of smaller organizations without a CRO, the ERC could consist of the chief information security officer (CISO) or the head of IT, the head of procurement, and the chief financial officer (CFO). The objective is to facilitate cross-departmental collaboration, regardless of the company's size.

# Process: Defining Who and What to Measure

## Step 1: Set Enterprise Objectives

With the ERC in place, the enterprise objectives for TPRM are then determined. The ERC begins by asking strategic questions, including:

- What are our objectives? What are we aiming to accomplish?
- Do we have any metrics in mind?
- Which regulations apply to us?
- Why is the business investing in this program?
- How can we demonstrate successful implementation of TPRM at scale?
- How do we track risk reduction success in the program over time?

Upon addressing these questions, the ERC then develops the enterprise objectives for TPRM, potentially utilizing a solution offered by a TPRM vendor. These may include:

- Protecting the organization's and customers' sensitive data and intellectual property
- Ensuring legal and regulatory compliance of vendors and suppliers
- Implementing measures to decrease cybersecurity risks
- Implementing measures to mitigate operational and financial risks
- Safeguarding the organization's reputation
- Enhancing the organization's operational efficiency
- Ensuring business resilience with a clear action plan, and ensuring team members understand their roles and responsibilities
- Implementing a TPRM program that supports informed decision-making

## TPRM Metrics Categories: An Overview

Before proceeding to set specific departmental objectives, it's important to have a clear understanding of the **different categories of TPRM metrics** that can be considered.

It's also essential at this point to understand the difference between KPIs and KRIs, as both are equally important to TPRM metrics.

- **Key Performance Indicators (KPIs)** measure the effectiveness of organizational processes and functions
- **Key Risk Indicators (KRIs)** measure the level of risk the organization faces and how effectively it's being managed

As part of a robust third-party risk management strategy, your organization should focus on four primary areas of measurement. Each area consists of KPIs and KRIs that provide invaluable insights into your relationship with suppliers.

- **Risk Metrics:** These metrics help in assessing the risks associated with specific suppliers. They provide insights into potential threats, corresponding mitigation strategies, and the supplier's adherence to both primary and remunerative controls.
- **Threat Metrics:** These metrics consist of publicly available data relating to cyber, operational, financial, and reputational aspects. They help to address how vendor risk data correlates with externally observable threats.
- **Compliance Metrics:** These metrics reveal how well suppliers' practices comply with your organization's internal control environment. They also measure adherence to regulatory requirements and frameworks, which is critical for maintaining legal and industry standards.
- **Coverage Metrics:** These metrics are designed to ensure that your organization has a complete understanding of its global supplier footprint. They help identify the third, fourth, and Nth parties in your supply chain and verify whether they have been classified appropriately in your program.

The first two categories, Risk and Threat Metrics, largely consist of KPI and KRI metrics related to risk factors and external influences. The latter two categories, Compliance and Coverage metrics, are geared more toward internal program evaluation and alignment. These four categories together provide a comprehensive and balanced approach to third-party risk management.

Now that we have an understanding of the different categories of TPRM metrics, we can proceed to establish objectives at the departmental level.

## Step 2: Set Departmental Objectives

During this phase, the CEO could meet with the departmental heads and invite them to the ERC. In smaller organizations, the CEO might meet with the CISO or the head of IT, head of procurement and the CFO. The departmental heads then define the departmental objectives for TPRM drawing from ERC recommendations.

Here are some of the questions they would consider:

- Which third-party interactions are involved in our department's operations?
- What sensitive data and systems in our department can third parties access?
- Which regulations govern our department (e.g., GDPR)?

Once this is completed, departmental teams are formed, led by the departmental heads. These teams will have several responsibilities that are highlighted in the following steps.

## Step 3: Identify Third Parties

The departmental teams begin by identifying third parties such as vendors, suppliers, contractors, logistics partners, cloud service providers, or others. At this stage, teams might work with procurement, accounts payable, or other internal teams that maintain a working list of vendors and suppliers to centralize those third parties for better governance.

## Step 4: Identify Risks to Measure

After the third parties have been identified, the teams determine potential risks associated with each party. These risks might include data breaches, reputational concerns, regulatory fines, financial solvency concerns, and supply chain disruptions.

**RECOMMENDATION:**

Your organization might be confronted with several supplier risks that you were previously not aware of. Find out what these different types of risks are and how to mitigate them by reading the blog: **Top Supplier Risks and What to Do About Them**

## Step 5: Identify Performance Indicators

Upon identifying third parties and potential risks, the teams create and establish performance indicators for regular monitoring.

The following section offers some insights into what defines a **good metric for TPRM**.

- **Data Availability/Quality:** This ensures that data is available for reporting and that teams can access a centralized repository of holistic vendor risk profiles.
- **Standardization/Consistency:** Harmonizing processes and views across business units regarding potential vendor risks can streamline operations.
- **Data Integration across Multiple Systems:** This refers to the consolidation and integration of platforms to provide a unified view of vendor risk across the organization.
- **Simplicity of Analysis:** Automating programmatic processes can help manage the large volume of data that needs to be analyzed.
- **Interpretation and Contextualization:** This involves understanding the audience and context to provide clear, succinct, and meaningful information.
- **Report Formatting and Communication:** The ability to distill, communicate and present data in a user-friendly format is crucial.
- **Timeliness and Frequency:** The capacity to continuously monitor vendors and understand risk developments in real time is paramount in any effective TPRM program.

Teams can also seek support and recommendations from your TPRM vendor at this stage. Experienced vendors typically offer libraries containing relevant content, playbooks, and other information to aid in identifying pertinent risks, tracking performance indicators, building reporting strategies, and addressing other concerns.

## Use These Tips to Avoid Common Pitfalls When Setting Up TPRM Metrics:

- **Avoid the "design by committee" situation:** Each working group responsible for TPRM may have a unique view on relevant metrics. Strive for an integrated, rather than a disjointed, approach.
- **Pay attention to your organization's unique needs:** Align the metrics with the objectives of your TPRM program to ensure they are appropriate and meaningful.
- **Avoid information overload:** Achieve alignment between teams on the specific data to be measured and how it should be used. Not all data is relevant or useful.
- **Don't assume that indicators are easily identified and tracked:** This process requires diligence and contract review to ensure all relevant data is captured.
- **Facilitate cross-functional collaboration:** Engage teams from various departments to review the metrics, ensuring a comprehensive perspective.
- **Avoid focusing too much on performance and not enough on risk:** Overemphasis on KPIs and insufficient attention to KRIs can lead to skewed insights.
- **Avoid over-reliance on a single metric:** A single metric does not fully represent the broader program; it's crucial to consider multiple measures.
- **Recognize that one size does not fit all:** Different metrics will apply differently to various situations, so avoid assuming uniformity.
- **Don't be afraid to get data from your vendors early in the process:** Early access to data aids in informed decision-making.
- **Don't view TPRM as a one-time initiative:** It's a continuous, dynamic process.

## Step 6: Harmonize Metrics Across the TPRM Lifecycle

In this step, the ERC collaborates with department heads and establishes working groups to align all the identified risks and performance indicators. The groups then work to standardize and synchronize metrics across each stage of the **Third-Party Vendor Risk Management Lifecycle**.

The following chart highlights select metrics that should be considered at each stage along with the department that would typically be involved:

| | | Relevant to These Cross-Functional Teams | | | | |
|---|---|---|---|---|---|---|
| **Third-Party Risk Lifecycle Stage** | **Select TPRM Metrics** | **IT Security** | **Procurement** | **Risk Management** | **Internal Audit & Compliance** | **Finance** |
| **1. Sourcing & Selection** | ▪ Number of Tier 1 suppliers that have not returned self-attestation<br>▪ Credit rating or other financial score<br>▪ Reputational score or adverse media exposure from external intelligence sources | ✓ | ✓ | | | ✓ |
| **2. Intake & Onboarding** | ▪ Number of suppliers in use without a detailed profile or information on the service or product utilized<br>▪ Number of suppliers that present a continued high risk following successful onboarding<br>▪ Mean Time to Onboard (MTTO)—the time taken from engagement to completion of initial due diligence risk assessment for new supplier | | ✓ | ✓ | | |
| **3. Score Inherent Risk** | ▪ % of suppliers that have completed, passed, and failed an initial onboarding inherent risk assessment<br>▪ Inherent risk from each security domain category (e.g., Access Control, Asset Management, Physical Security, etc.) within supply chain<br>▪ Number of suppliers receiving payment that do not have an onboarded status | ✓ | ✓ | | | ✓ |
| **4. Assess & Remediate** | ▪ Mean time to complete supplier assessments<br>▪ Residual risk (after the application of controls) from each security domain category (e.g., Access Control, Asset Management, Physical Security, etc.) within supply chain<br>▪ Quality of compliance returns from suppliers by Tier (1,2,3,4) | ✓ | | | ✓ | |

| Third-Party Risk Lifecycle Stage | Select TPRM Metrics | Relevant to These Cross-Functional Teams: IT Security | Procurement | Risk Management | Internal Audit & Compliance | Finance |
|---|---|---|---|---|---|---|
| **5. Monitor & Validate** | ▪ % difference between supplier self-attestation and threats based on intelligence sources<br>▪ Accuracy of threat intelligence source as measured by the number of false positives/number of alerts (reported as a %)<br>▪ Number of Tier (1,2,3,4) suppliers with active "high" threat intelligence indicators | ✓ | ✓ | | | |
| **6. Manage Ongoing Performance** | ▪ Number of priority 1 security incidents generated from supply chain in the last quarter<br>▪ Number of vendors within supply chain with a high-risk score<br>▪ % coverage of the supply chain globally | ✓ | ✓ | ✓ | | |
| **7. Terminate & Offboard** | ▪ Number of suppliers within all tiers that have outstanding threat intelligence or control deficiencies not under effective management<br>▪ Number of suppliers that are categorized as in scope for a compliance program (e.g., SOX, PCI, GDPR)<br>▪ Number of suppliers outside of Tier 1 with compliance obligations | ✓ | ✓ | ✓ | ✓ | |

**RECOMMENDATION:**

To find out more about how to identify the right TPRM metrics, read the eBook **"The 25 Most Important KPIs and KRIs for Third-Party Risk Management"** and download the **scorecard**.

# The Mitratech TPRM Solution

Whether you are starting a new TPRM program or want to optimize your existing TPRM metrics initiatives, Mitratech can provide the solutions, services and support you need.

The Mitratech Third-Party Risk Management Platform is a SaaS solution that can enable your entire organization to collaborate on identifying, understanding and reducing vendor risk. With the Mitratech platform, you can:

- **Build a centralized database of vendor and supplier risk profiles,** including mapping 4th and Nth-party relationships
- **Automate the third-party risk assessment process** with a library of over 200 standardized questionnaires
- **Continuously monitor** for new and emerging cyber, financial, operational, and reputational risks
- **Manage and track the remediation process** with automated workflow and playbook capabilities with stakeholders throughout the organization

This is backed by our experienced professional services (PS) team, who can help you further streamline the process by:

- Helping to identify pertinent KPI and KRI metrics across the vendor lifecycle
- Establishing threshold expectations and initiating timely alerts
- Supporting you throughout the remediation process, as well as tracking resolution procedures
- Providing access to a comprehensive library of TPRM content, specifically around custom reporting, TPRM programs, and related performance criteria
- Working with you to develop custom reports tailored to various stakeholders
- Supplying your teams with essential support and documentation based on various persona-based status workflows

To get started with measuring key metrics, **download the eBook** and **scorecard**, The 25 Most Important KPIs and KRIs for Third-Party Risk Management. Then, **schedule a demo** to learn how Mitratech can help you automate and accelerate your TPRM metrics program.

## About Mitratech Third-Party Risk Management

Mitratech is a proven global technology partner for legal, risk, compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility, and spurring collaboration across an enterprise.

Mitratech takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers, and other third parties across the entire vendor lifecycle. Our clients benefit from a flexible, hybrid approach to TPRM, not only gaining solutions tailored to their needs, but also realizing a rapid return on investment. Regardless of where they start, we help our clients stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.
Mitratech serves over 24,000 organizations worldwide, spanning more than 160 countries.

To learn more, please visit: **www.mitratech.com**.