Prevalent™

The 25 Most Important KPIs and KRIs for Third-Party Risk Management

How to Measure and Communicate TPRM Program Effectiveness to the Board

Table of Contents

Introduction

With the unprecedented growth of vendor data breaches and supply chain disruptions, boards of directors and company leaders are craving greater visibility into their third-party ecosystems.

The problem is, few security and risk professionals know how to effectively communicate third-party risk – often relying on complex, technical and point-in-time dashboards that lead to board confusion and/or disengagement.

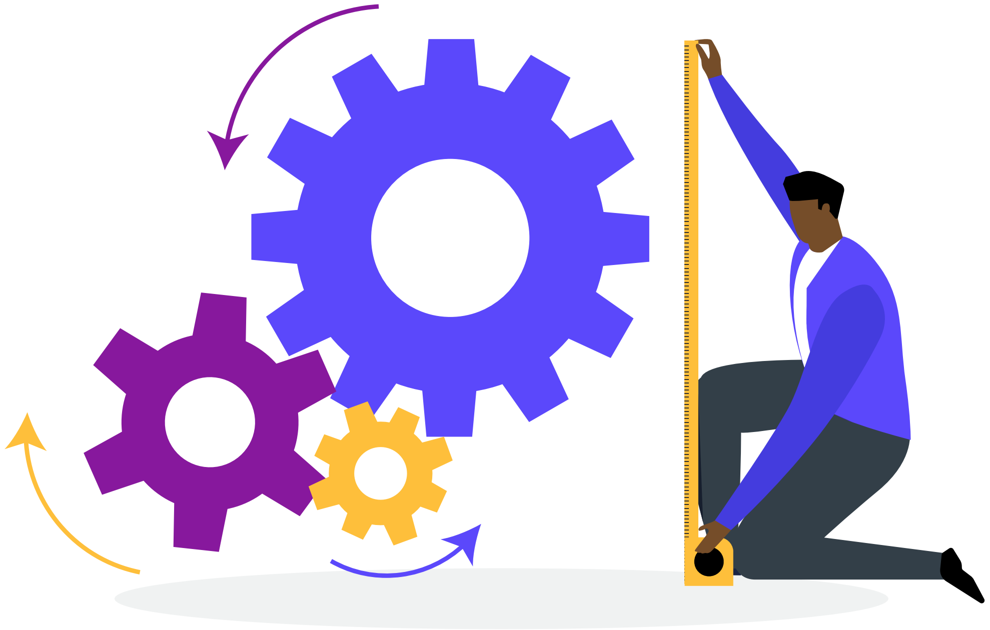
How can CISOs effectively communicate third-party risk to the board?

1. Speak the language of the board: risk and its financial impact
2. Provide a concise, high-level view of meaningful, near real-time metrics

This eBook will get you started by:

- Clarifying the difference between KPIs and KRIs
- Identifying four categories of metrics to measure
- Recommending 25 KPIs and KRIs to report to the board and leadership
- Revealing which types of metrics are best for CISOs, business leadership and the board

The Difference Between KPIs and KRIs



Key Performance Indicators (KPIs) measure the effectiveness of functions and processes.

Key Risk Indicators (KRIs) measure how much risk the organization faces and which risk treatments to apply.

Both are equally important in measuring the people-process-technology triad.

Four Key Metrics Categories

For third-party risk management, your organization should measure four areas. Each area includes KPIs and KRIs.

Quantified and Balanced Risk

Data on primary and compensatory controls

Risk

What is the risk of doing business with each third party and what mitigations are required?

External Threat Intelligence

Publicly available intelligence (cyber, business, financial, reputational)

Threat

How does vendor risk data correlate with externally observable threats?

Context-driven Compliance

Adherence to regulations and frameworks

Compliance

Is the third party meeting compliance requirements in the context of our internal control environment?

Global View, Local Lens

Supplier relationship mapping and categorization

Coverage

Who are the fourth and Nth parties in our supply chain, and are suppliers tiered appropriately for our program?

Risk Metrics

Key Performance Indicator	What It Means
% of suppliers by Tier (1,2,3,4)	Segments the supplier base to provide a high-level understanding of criticality.
% of suppliers that have completed an initial onboarding inherent risk assessment	A low percentage of suppliers in this KPI could mean the company is exposed to unknown risks at the earliest stage of the relationship.
Number of suppliers that have passed/failed the initial onboarding inherent risk assessment	A high number of suppliers in this KPI provides guidance on which are the riskiest and require more comprehensive risk assessments and ongoing monitoring.
Mean time to complete supplier assessments	A long time to complete assessments could indicate supplier disengagement or that the assessment is too complicated according to their Tier.

Key Risk Indicator	What It Means
Number of priority 1 security incidents generated from supply chain in the last quarter	More of a lagging indicator, if this KRI is trending upward you may need to expand the scope of your cybersecurity assessments or implement continuous monitoring to stay on top of emerging risks.
Number of vendors within supply chain with a high risk score	A leading indicator, this KRI enables you to prioritize due diligence on the riskiest suppliers.
Number of suppliers that present a continued high risk following successful onboarding	A high number would indicate that suppliers did not follow through on recommended remediations; the business could look to the contract for enforcement measures, consider compensating controls, or accept the risk.
Inherent risk from each security domain category (e.g., Access Control, Asset Management, Physical Security, etc.) within supply chain	Helps to determine which security domains require further due diligence and monitoring efforts above and beyond the baseline set of controls.
Residual risk (after the application of controls) from each security domain category (e.g., Access Control, Asset Management, Physical Security, etc.) within supply chain	A high level of residual risk could require the company to consider compensating controls, accept the risk, or seek to exit the contract.

Threat Metrics

Key Performance Indicator	What It Means
% coverage of supplier base by Tier (1,2,3,4) with threat intelligence	A low percentage of top-tier suppliers (e.g., Tier 1) monitored by threat intelligence means that some of your most critical vendors only have periodic (for example, annual) assessments completed against them – which creates a risky gap in supplier insights.
Mean Time to Action (MTTA) for risk owner after threat intelligence trigger	A high MTTA could indicate that the risk owner is overwhelmed by noise, making it difficult to find the events that require investigation. Could also be a skills gap or a complex threat to investigate.
Accuracy of threat intelligence source as measured by the number of false positives/number of alerts (reported as a %)	A high percentage of false positives would require alert threshold tuning or further investigation into the threat intelligence source.

Key Risk Indicator	What It Means
% difference between supplier self-attestation and threats based on intelligence sources	A high percentage of intelligence findings in conflict with assessment answers could indicate that the supplier is not accurately responding to their assessments. Could trigger a re-assessment or supplementary assessment requiring additional supporting evidence.
Number of Tier (1,2,3,4) suppliers with active "high" threat intelligence indicators	A large number could indicate that your supplier base is ripe for cyber-attack or actively under attack. Recommend targeted supplementary risk assessments to measure the effectiveness of supplier internal controls to withstand such attacks.
Mean Time to Resolve (MTTR) for Tier (1,2,3,4) threat indicators	Similar to the MTTA KPI above, a high MTTR could indicate a skills gap or a complex threat to investigate. High MTTR might require engaging outside security specialists or a supplier contractual review to ensure they are following appropriate procedures to mitigate threats.

Compliance Metrics

Key Performance Indicator	What It Means
Number of suppliers that are categorized as in scope for a compliance program (e.g., SOX, PCI, GDPR)	A high number of suppliers requiring specific compliance assessments will show how much scrutiny should be paid to the regulation at hand, for example data privacy.
Quality of compliance returns from suppliers by Tier (1,2,3,4)	A high percentage of unanswered or mis-answered questions (e.g., low quality) can extend assessment timelines and remediation. May require supplementary assessments requiring specific evidence or controls validation performed by an outside auditor.

Key Risk Indicator	What It Means
Number of suppliers outside of Tier 1 with compliance obligations	A greater level of scrutiny is typically applied to Tier 1 suppliers, but a large number of non-Tier 1 suppliers with compliance obligations may require supplementary regulatory-specific assessments to measure adherence to requirements.
Number of suppliers within all tiers that have outstanding threat intelligence or control deficiencies not under effective management	A large number indicates a high level of risk. Outstanding control deficiencies and threat intelligence findings should be addressed according to priorities and risk tolerance thresholds.

Coverage Metrics

Key Performance Indicator	What It Means
% coverage of the supply chain globally	A low percentage of suppliers actively managed, assessed or monitored by the organizations indicates a higher level of risk that the company is exposed to. All suppliers should be tiered, categorized, and managed accordingly.
Number of suppliers receiving payment that do not have an onboarded status	A high number here indicates a lapse of enforcement in the supplier due diligence process (or no process at all). Without proper onboarding – including an inherent risk assessment – the company is exposed to security, operational, contractual, and financial risks.
Mean Time to Onboard (MTTO) – the time taken from engagement to completion of initial due diligence risk assessment for new supplier	A short time to complete a new supplier onboarding assessment could mean that the questionnaire is not comprehensive enough and you could be missing important risk metrics. On the other hand, a long time to complete initial due diligence could indicate that the assessment is too complex. Review the assessment to ensure the right information is being gathered for the supplier's place in the third-party lifecycle.

Key Risk Indicator	What It Means
Number of suppliers in use without a detailed profile or information on the service or product utilized	A high number of suppliers here means that a comprehensive vendor profile has not been built, and important information such as demographics, fourth-party technologies in use, financial information and more has not been considered as part of the risk assessment process. Conduct a detailed profiling and tiering assessment to gather this information.
Number of Tier 1 suppliers that have not returned self-attestation	A high number of suppliers here means that you have little visibility into the internal controls that the most critical suppliers have implemented to protect access to your systems and data, which is quite risky. Chasing services are available to help speed up the collecting and analysis of supplier self-attestations.
Number of Tier 1 suppliers not covered by threat intelligence	A high number of suppliers here means that you are missing key near real-time insights into cybersecurity, business, reputational and financial risks that can impact your company. The combination of assessments and threat intelligence information helps to validate the effectiveness of certain controls.

Sharing the Right Metrics with the Right Stakeholders

Use this guidance to present the right metrics to the right stakeholders.

CISO

- Deliver an in-depth review showing compliance adherence for all suppliers in all tiers
- Present a threat intelligence deep dive detailing inherent and residual risk for each supplier in all tiers
- Prioritize action and remediation plans for all identified issues

Business

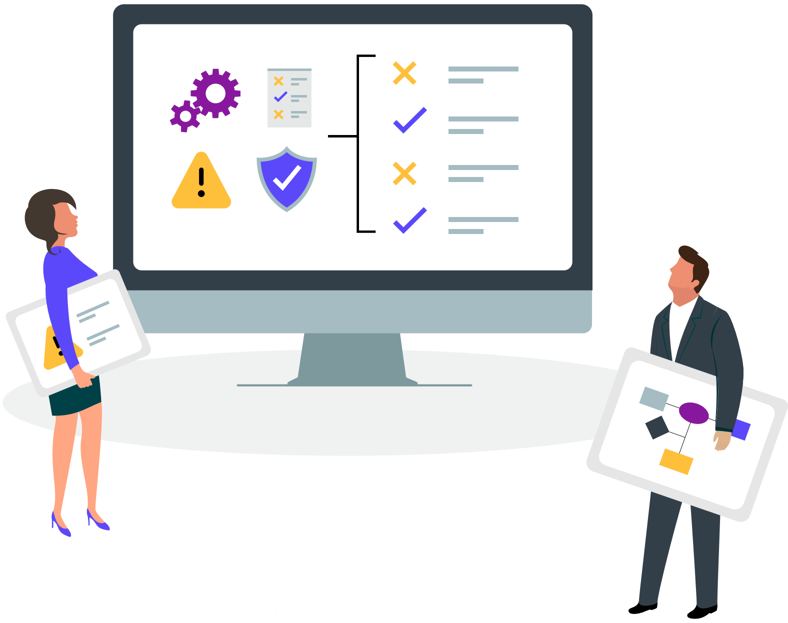
- Show business users near real-time threat/risk analysis for their suppliers
- Conduct proactive deep dives for Tier 1 and critical Tier 2 suppliers to improve supplier relationships
- Identify a clear action plan to drive remediation and resolution of identified issues

Board

- Present a consolidated view of current risk exposure to the organization from the supply chain
- Communicate current status of critical suppliers supporting major company efforts
- Show inherent and residual risk from threat intelligence sources to demonstrate progress in reducing risk over time
- Identify where executive support is needed

Getting Started with KPIs and KRIs for Third-Party Risk Management

Effectively reducing third-party risk requires an understanding of how people, processes and technology are performing against expectations. However, traditional vendor risk management products are unable to deliver the visibility necessary to manage and track performance and risk across the vendor lifecycle.



Prevalent can help simplify the measurement of risk and program effectiveness by:

- Identifying KPIs and KRIs to manage throughout the vendor lifecycle as part of the initial contracting process
- Detecting threshold exceptions and sending alerts
- Providing remediation guidance and tracking the resolution process
- Delivering customizable reporting for multiple stakeholders

Download the KPI/KRI Scorecard (.xlsx) to get a head start on managing key metrics or request a demo and strategy discussion today!

About Prevalent

Prevalent 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 and suppliers throughout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

Visit **www.prevalent.net** to learn more.