Gartner®

Enterprise Third-Party Risk Management

Published 18 May 2023 - ID G00778074 - 16 min read

By Analyst(s): Jonathan Keeney

Initiatives: Risk Response Strategies

Heads of enterprise risk management are spending much more time managing third-party risk than previously, but their efforts are not correspondingly impacting outcomes. They must follow our three imperatives to prioritize enterprise third-party risks more effectively.

More on This Topic
This is part of an in-depth collection of research. See the collection:

- Top Resources for 2023 ERM Priorities

Overview

Exposure to third-party risk has exploded in recent years. To avoid costly third-party incidents, enterprise leaders are asking ERM to play a greater role in third-party risk management (TPRM).

Our research shows that heads of ERM view prioritization as their most important job regarding third-party risk. They know their stakeholders need them to assess the many third-party risk issues and focus attention on those that are most important for the enterprise as a whole. But knowing the right goal is only half the battle, and for many ERM teams today, effectively prioritizing third-party risk remains elusive. In this research, we identify three imperatives to help ERM overcome common challenges and achieve enterprise TPRM.

Key Findings

- Third-party risk has become a more important priority for ERM. Seventy-six percent of executive risk committee members say their committee places greater emphasis on third-party risk, and 78% say their expectations of ERM regarding third-party risk have grown.
- ERM teams struggle to prioritize third-party risks. Only a minority of heads of ERM say they are concise (26%), prioritized (19%) and actionable (16%) in the view of third-party risk they present to stakeholders.
- While ERM teams have roughly doubled their level of involvement in TPRM activities since 2016, increased involvement has not delivered the desired results. Greater involvement in TPRM activities does not improve ERM's prioritization ability and only modestly improves third-party risk outcomes.
- In contrast, ERM teams that effectively follow an "enterprise TPRM" approach significantly improve their ability to prioritize third-party risks and the organization's third-party risk outcomes.

This document was revised on 12 October 2023. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

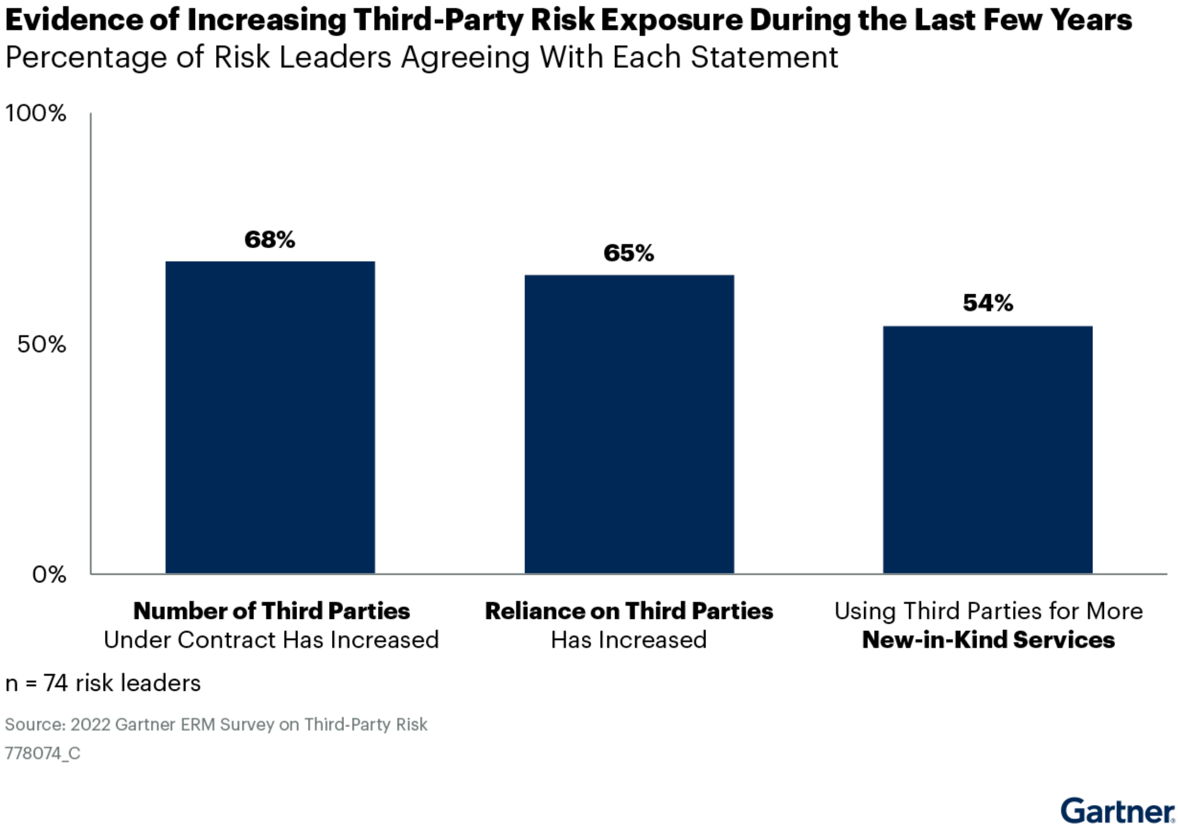
ERM Must Address the Third-Party Risk Boom

Organizations are experiencing a surge in their exposure to third-party risk. In the 2022 Gartner ERM Survey on Third-Party Risk, risk leaders said their organizations are working with more third parties (68%), relying more on those third parties (65%) and using third parties for a greater array of services (54%) than they were just a few short years ago (see Figure 1). [1] These organizations are also navigating an unprecedented period of simultaneous major disruptions, which include:

- Supply chain disruption
- Russia's invasion of Ukraine
- Cybercrime
- Persistent inflation

These disruptions continue to have massive, cascading effects across organizations' third-party networks.

Figure 1: Evidence of Increasing Third-Party Risk Exposure During the Last Few Years



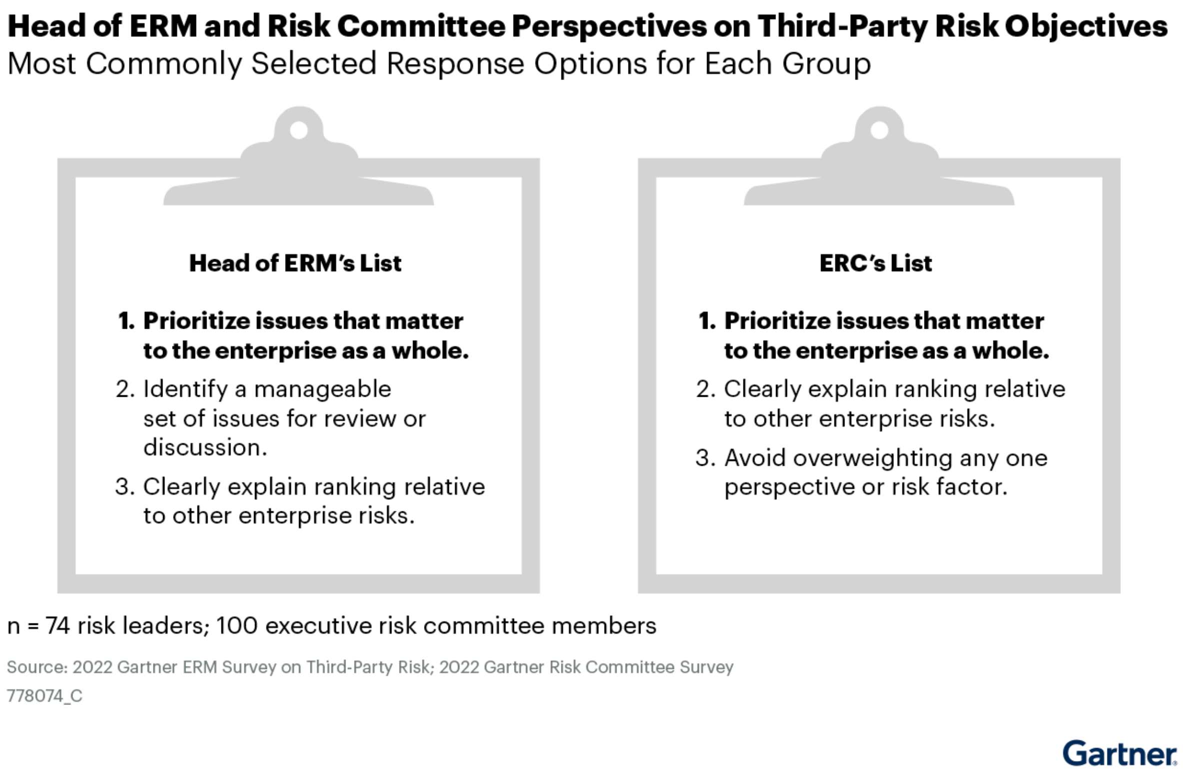
Source: 2022 Gartner ERM Survey on Third-Party Risk
778074_C

Accordingly, third-party risk has taken on greater importance for enterprise leaders tasked with managing risk. In the 2022 Gartner Risk Committee Survey, 76% of respondents said third-party risk had become a more important priority for their executive risk committee (ERC). No one disagreed with the statement. In the same survey, 78% of respondents said their expectations of their ERM team concerning third-party risk had also increased. [2]

Heads of ERM and ERC Members Agree on the Importance of Prioritization

Fortunately, some good news exists. Heads of ERM and ERC members agree that prioritization is ERM's most important job regarding third-party risk (see Figure 2). Heads of ERM correctly recognize that their stakeholders want them to accurately prioritize the many third-party risk issues facing the enterprise and to focus attention on the most impactful issues for the enterprise as a whole.

Figure 2: Head of ERM and Risk Committee Perspectives on Third-Party Risk Objectives



Head of ERM and Risk Committee Perspectives on Third-Party Risk Objectives
Most Commonly Selected Response Options for Each Group

Head of ERM's List

1. **Prioritize issues that matter to the enterprise as a whole.**
2. Identify a manageable set of issues for review or discussion.
3. Clearly explain ranking relative to other enterprise risks.

ERC's List

1. **Prioritize issues that matter to the enterprise as a whole.**
2. Clearly explain ranking relative to other enterprise risks.
3. Avoid overweighting any one perspective or risk factor.

n = 74 risk leaders; 100 executive risk committee members

Source: 2022 Gartner ERM Survey on Third-Party Risk; 2022 Gartner Risk Committee Survey
778074_C

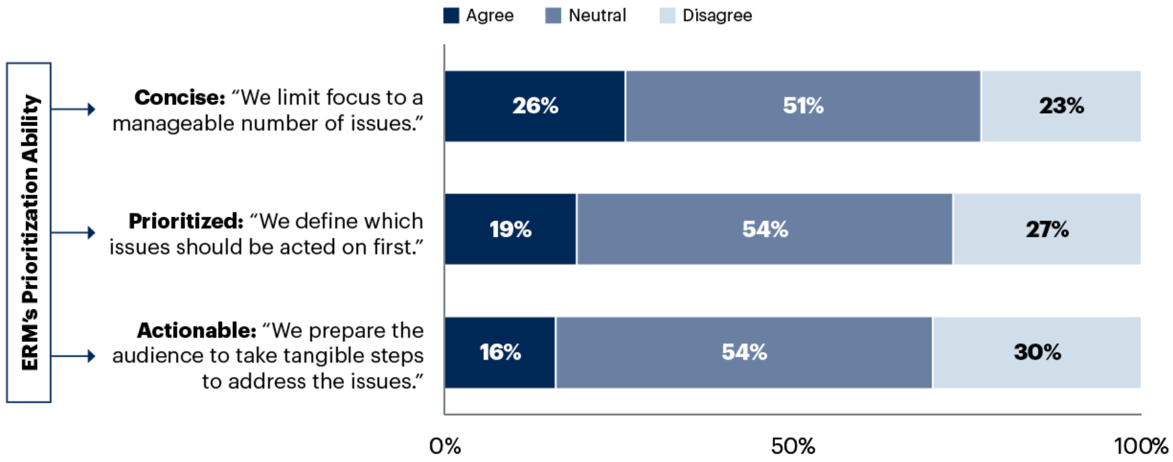
Gartner

ERM Must Become Better at Prioritizing Third-Party Risk Issues

Although heads of ERM know what they need to do, more than 70% of surveyed risk leaders indicated they did not always prioritize third-party risk issues effectively (see Figure 3). They must become better at giving the ERC a manageable number of issues to focus on, categorizing issues by relative importance and preparing ERC members to take action. For example, risk leaders might need to focus ERC members and other stakeholders on:

- A particular type of third-party risk (e.g., third-party cybersecurity risk)
- A particular type of third party (e.g., suppliers with operations in a conflict region)
- An individual third-party relationship (e.g., a critical third party with elevated risk and/or inadequate internal controls)
- A particular part of the business (e.g., a business unit with substandard TPRM procedures and/or compliance)

Figure 3: Difficulty Prioritizing Enterprise-Level Third-Party Risk Issues



Difficulty Prioritizing Enterprise-Level Third-Party Risk Issues
Percentage of Respondents[a]

n = 74 risk leaders

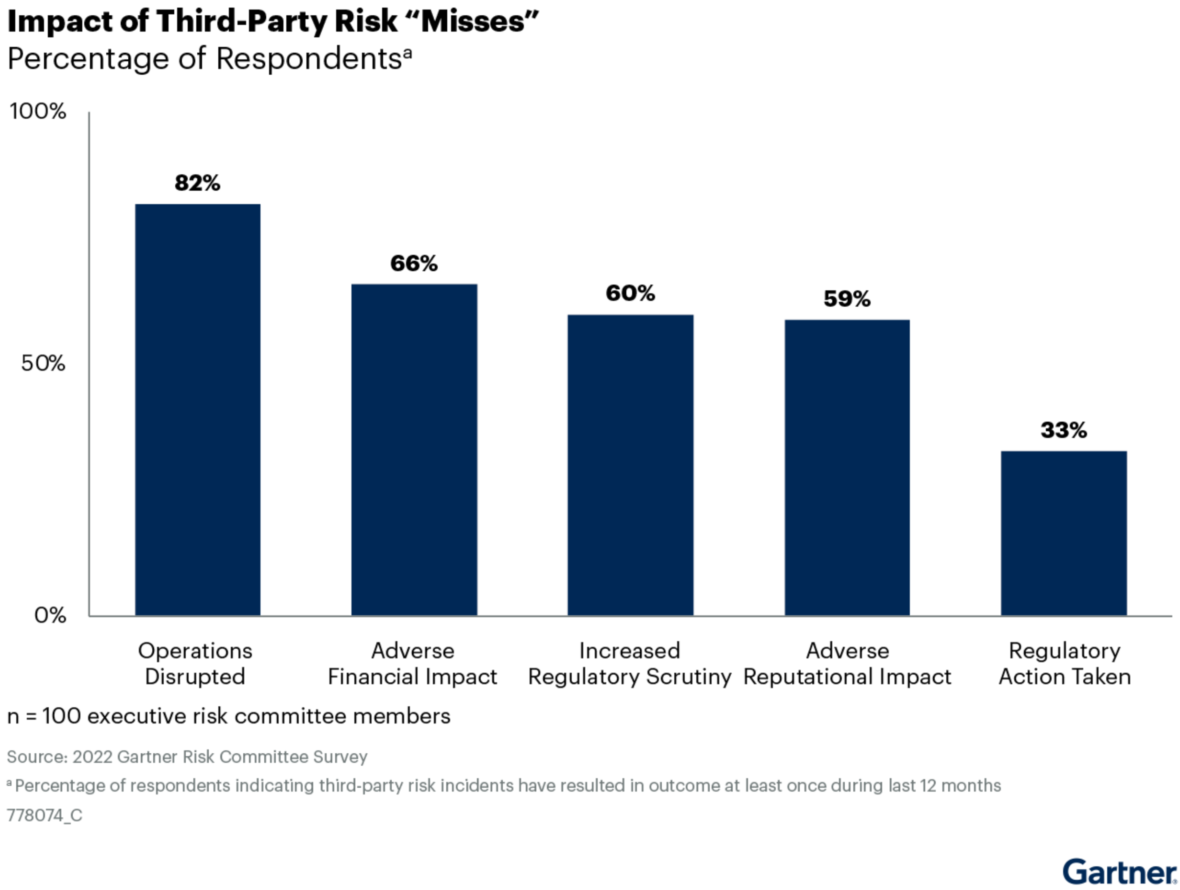
Source: 2022 Gartner ERM Survey on Third-Party Risk

[a] Percentage of respondents who agree they consistently achieve the following criteria in discussions of third-party risk with the risk committee, board and/or other senior executives

778074_C

Most organizations are suffering from the effects of third-party risk incidents. Our survey of risk leaders found that the operations of 84% of organizations had been disrupted at least once in the previous year because of a third party (see Figure 4). Furthermore, regulators had taken action against a third of respondents' organizations. These organizations would benefit greatly if ERM did a better job helping them manage third-party risk.

Figure 4: Impact of Third-Party Risk "Misses"



n = 100 executive risk committee members

Source: 2022 Gartner Risk Committee Survey

[a] Percentage of respondents indicating third-party risk incidents have resulted in outcome at least once during last 12 months

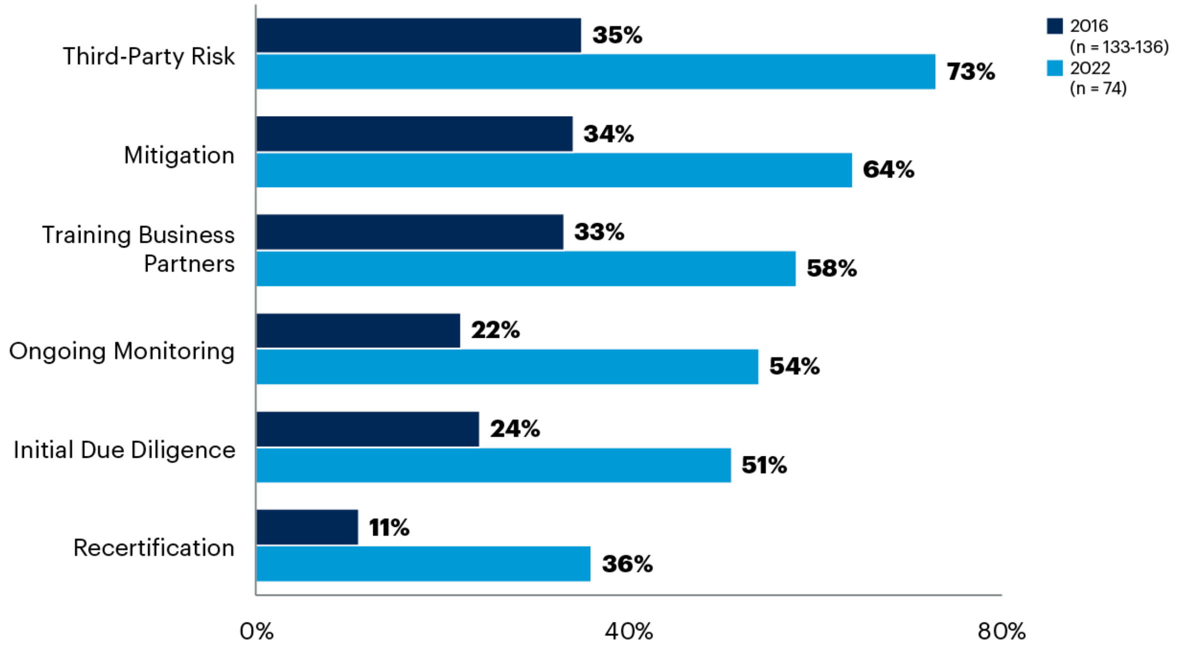
778074_C

Third-Party Risk Requires Different Management Tactics

Heads of ERM know they must become better at prioritizing third-party risk, but they have no consensus on what they should do differently to achieve that goal. Our surveys show that heads of ERM have been trying to tackle the problem by becoming much more involved in a broad range of TPRM activities (see Figure 5). These activities would typically be owned by compliance, procurement, a dedicated TPRM team or even the legal department.

Figure 5: ERM Involvement in Third-Party Risk Management Activities, 2016 vs. 2022

ERM Involvement in Third-Party Risk Management Activities, 2016 vs. 2022
Percentage of Respondents



n = varies, risk leaders

Source: 2016 Gartner State of the ERM Function Survey; 2022 Gartner ERM Survey on Third-Party Risk
778074_C

However, ERM teams that spend significantly more time on TPRM activities are no better at prioritizing third-party risk issues. They still have much to do to develop the “prioritization ability” (the ability to have a concise, prioritized and actionable view of third-party risk at the enterprise level). Developing this is vital to focusing on the most important issues and not becoming distracted by less important ones. Indeed, ERM simply spending more time on TPRM activities only results in a modest 25% increase to their organizations’ overall TPRM effectiveness. [1]

ERM must use different tactics when managing third-party risk than when managing other types of risk. Table 1 shows the typical roles ERM plays in managing a range of risks (such as cybersecurity risk, financial risk and talent risk). But third-party risk also has several unique characteristics. ERM’s typical aggregator, thought partner and trend spotter roles prove less effective for managing third-party risk.

Table 1: Typical ERM Roles Versus Characteristics of Third-Party Risk

Typical ERM Role	Characteristic of Third-Party Risk That Makes ERM Role Less Effective
Aggregator: Combines inputs from across the business to determine what's most important	Many heterogeneous risks that vary greatly in importance across the business are combined.
Thought Partner: Spends time with risk owners to identify key issues and test what matters most to them	Risk ownership is naturally distributed among many different people/functions.
Trend Spotter: Uses subject matter expert perspective or data to anticipate emerging issues in the risk landscape	Issues are too numerous and diverse; available data is point-in-time and lagged.

Source: Gartner

ERM's aggregator role does not work with third-party risk because this type of risk is composed of a wide array of heterogeneous elements, such as third-party impacts on the organization's:

- Reputation
- Financial performance
- Ability to maintain continuous supply and operations
- Cybersecurity
- Data privacy

It is not possible to aggregate such diverse impacts into a single meaningful data point. Likewise, ERM's typical thought partner role is not well-suited to third-party risk either. Most enterprise risks have a single risk owner, but because third-party risk is so vast and varied, different groups and roles are responsible for different parts of the risk. This means third-party risk has no overarching owner with whom ERM can act as a thought partner. This poses a big coordination challenge.

Similarly, ERM's trend spotter role is not well-suited to third-party risk. The elements of third-party risk are far too varied, and most relevant data for understanding them is already old by the time ERM examines it, so it is not useful for predictive purposes. For example, usually someone in compliance performs a due diligence process when contracting with and onboarding a third party. The questionnaire this person completes at onboarding often contains the data points the organization uses to assess third-party risk. These will not remain relevant for very long after onboarding and certainly will not be useful for forward-looking analysis.

Three Imperatives for Managing Third-Party Risk

To develop and maintain a prioritized, enterprise-level view of third-party risk, heads of ERM must:

- **Define enterprise-level priorities.** Play more of a role in identifying enterprise-level priorities to aggregate third-party risk at the enterprise level. For example, determine whether third-party cybersecurity risk is more important than third-party financial risk, and rank order priorities appropriately.
- **Enable cross-functional alignment.** Do more to align and coordinate the many disparate groups or functions involved in third-party risk.
- **Monitor forward-looking indicators.** Find and track forward-looking indicators on third-party risk to focus analysis on the most critical emerging issues in the third-party risk landscape.

In many organizations, it is unclear what ERM's unique value-add is in managing third-party risk. But our three imperatives combine to form what we call enterprise third-party risk management (E-TPRM). ERM is uniquely positioned to provide this enterprise-level view of third-party risk, which enterprise leaders desperately need (see Table 2).

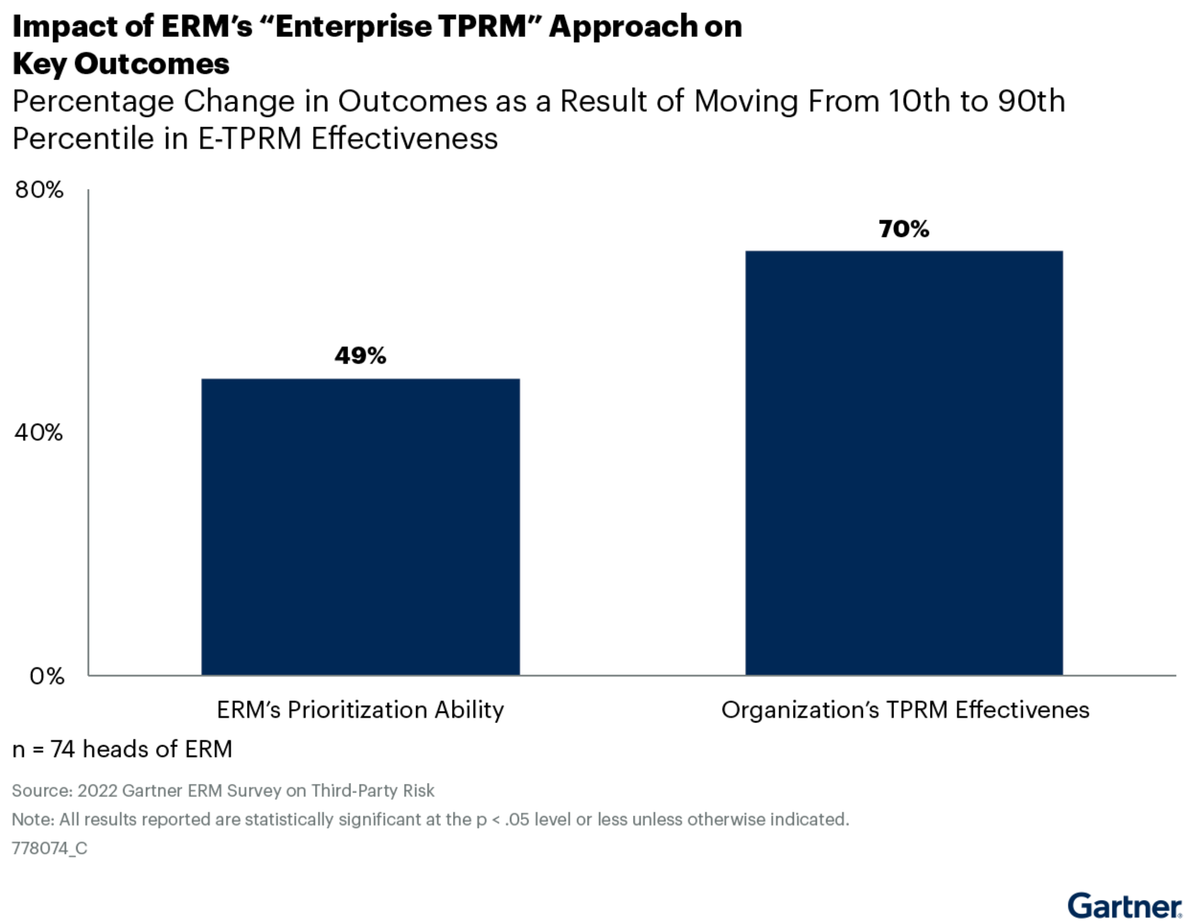
Table 2: The Three Imperatives of E-TPRM for Heads of ERM

Imperative for ERM	What It Means	Why It Works
Define enterprise-level priorities	Isolate and combine **only those inputs that matter most** at the enterprise level.	With an explicit, shared set of priorities, ERM can aggregate the inputs that matter most to the enterprise.
Enable cross-functional alignment	Help risk co-owners **obtain a holistic view** and create opportunities for them to work toward **consensus.**	By facilitating thought partnership among risk co-owners, ERM uses diverse expertise and aligns action.
Monitor forward-looking indicators	**Limit focus** to the most critical emerging issues and **track** them.	A focused set of easily monitored indicators enables ERM to reliably spot enterprise-critical trends.

Source: Gartner

When heads of ERM adopt E-TPRM, it has a big impact on ERM's ability to maintain and share a concise, prioritized, actionable view of third-party risk at the enterprise level (see Figure 6). In addition, it has a massive impact on the organization's overall effectiveness in managing third-party risk.

Figure 6: Impact of ERM's "Enterprise TPRMt" Approach on Key Outcomes



Impact of ERM's "Enterprise TPRM" Approach on Key Outcomes

Percentage Change in Outcomes as a Result of Moving From 10th to 90th Percentile in E-TPRM Effectiveness

n = 74 heads of ERM

Source: 2022 Gartner ERM Survey on Third-Party Risk

Note: All results reported are statistically significant at the p < .05 level or less unless otherwise indicated.

778074_C

Implementing our three imperatives for E-TPRM can be challenging. In the following sections, we describe those challenges and provide high-level solutions, illustrated with specific examples from leading ERM teams.

Define Enterprise-Level Priorities

Defining enterprise-level priorities can be difficult because it is hard to isolate and combine only those inputs that matter most at the enterprise level for third-party risk. The many heterogeneous subrisks that third-party risk encompasses vary greatly in their relevance to different parts of the business. This makes it difficult to distill clear priorities using a traditional, "bottom up" approach.

Overcome this challenge by developing a scoring framework based on enterprise-level risk factors to consistently assess the risk posed by individual third parties and prioritize risk actions.

Case in Point: Enterprise Third-Party Risk Prioritization Framework (Empire Life)

Empire Life

To establish a consistent, enterprisewide methodology of assessing third-party risk and prioritizing third-party risk response actions, the head of ERM at Empire Life developed an enterprise third-party risk prioritization framework. ERM first identifies the various risks that can be driven by or through third parties. Those risks are then filtered down to a shortlist of those factors that matter most to the enterprise by applying a standard set of criteria (including the extent to which risks are cross-functional, related to strategy enablement and related to regulatory requirements) and weighed to reflect their relative importance (see Figure 7).

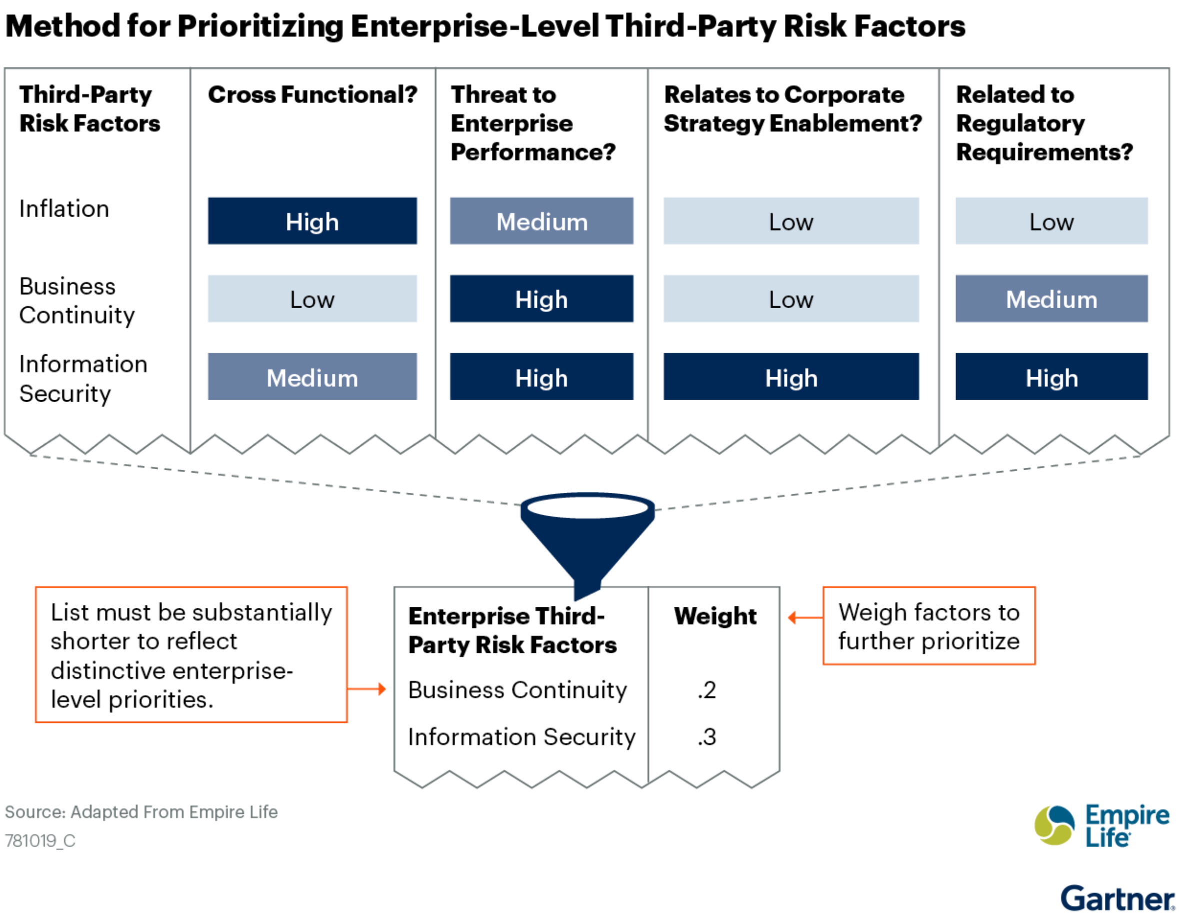
Empire Life then uses these weighted risk factors to calculate residual risk scores for each major third party. ERM uses existing data sources (e.g., due diligence and other compliance surveys) to select proxy questions reflecting inherent risk and control effectiveness for each risk factor. The difference of these two scores (residual risk) provides a consistent metric that can be used to highlight gaps and prioritize where action is needed most.

Specifically, Empire Life uses the residual risk ratings for individual third parties to anchor key stakeholder conversations, resulting in a prioritized list of third-party actions. These include conversations with business unit heads to find the root cause of prioritization discrepancies, and with the risk committee, using data to identify trends and outliers.

With no costs beyond the initial investment of staff time to set up the framework, this approach has improved Empire Life's ability to focus ERM's efforts, and the ERC's attention, on the third-party relationships that matter most from an enterprise perspective and to drive third-party risk awareness across the enterprise.

For more details, see Case Study: Rate Third-Parties at the Enterprise Level for Risk-Based Prioritization.

FIgure 7: Method for Prioritizing Enterprise-Level Third-Party Risk Factors



Method for Prioritizing Enterprise-Level Third-Party Risk Factors

Third-Party Risk Factors	Cross Functional?	Threat to Enterprise Performance?	Relates to Corporate Strategy Enablement?	Related to Regulatory Requirements?
Inflation	High	Medium	Low	Low
Business Continuity	Low	High	Low	Medium
Information Security	Medium	High	High	High

List must be substantially shorter to reflect distinctive enterprise-level priorities.

Enterprise Third-Party Risk Factors	Weight
Business Continuity	.2
Information Security	.3

Weigh factors to further prioritize

Source: Adapted From Empire Life

781019_C

Enable Cross-Functional Alignment

It's hard to align action on shared issues among the many stakeholders involved in managing third-party risk. This is because differences in perspective, type and level of expertise and functional priorities prevent the various co-owners of third-party risk from arriving at a shared view of the highest-priority enterprise-level issues and acting to resolve them. Differences in decision-making authority further complicate the picture, as subject matter experts with the greatest awareness and understanding of specific third-party risk issues often lack the authority to act on those issues.

Solve this problem by holding cross-functional discussions of third-party risk that break down functional silos. By engaging expertise and authority at appropriate moments in the process, ERM can fulfill its mandate to get risk information from the informed to the empowered in a timely manner.

Case in Point: Enable Cross-Functional Alignment to Prioritize Third-Party Risks (Blue Cross NC)

Blue Cross and Blue Shield of North Carolina (Blue Cross NC) aligns cross-functional perspectives on third-party risk through an expert-led risk calibration process. Subject matter experts from different assurance functions with a role in managing third-party risk (i.e., security, privacy, audit, risk and compliance) meet monthly to discuss Blue Cross NC's most critical and at-risk third-party relationships. These monthly meetings allow experts to align their perspectives, prioritize new issues, monitor progress on previously identified issues and take any necessary immediate actions. Once a quarter, senior executives from each function assemble to review and resolve any issues that can't be addressed through the monthly meetings — for instance, issues requiring a more senior-level perspective or greater decision-making authority.

To prepare experts to have impactful conversations each month, Blue Cross NC circulates a dashboard prior to each meeting that includes each function's rating of each key third party (using a simple red/yellow/green scale; see Figure 8). Experts are expected to review the dashboard and answer a set of prep questions prior to attending the meeting to ensure they arrive prepared to have an enterprise-level conversation. The prep questions focus experts on trends and broader patterns in the dashboard (e.g., "Do any of your peers' ratings make you think a particular vendor is riskier than your initial assessment showed?").

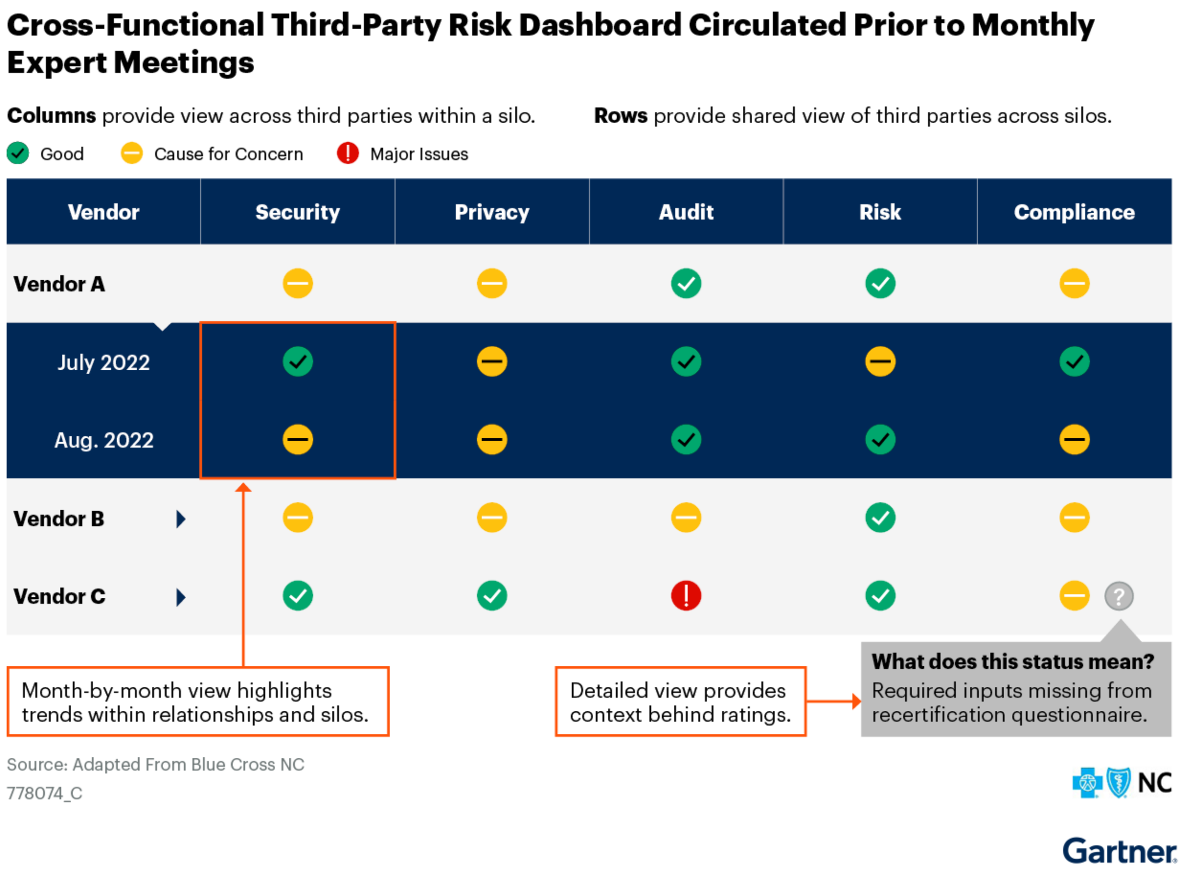
The monthly meeting agenda prioritizes issues that are likely to have a broader impact across the enterprise, including:

- Systemic issues with individual third parties (i.e., third parties rated poorly across multiple functions)
- Systemic issues within a function (i.e., multiple third parties rated poorly by an individual function)
- Seemingly isolated but significant issues (i.e., "red" ratings on the dashboard that might have potential for contagion)
- Trending issues across multiple vendors (i.e., declining ratings in multiple places on the dashboard that could indicate a worrying trend)

Experts discuss these issues to determine which to prioritize, which the experts can resolve themselves and which to escalate to the quarterly executive meeting.

> Since implementing this approach, Blue Cross NC has reduced the number of third parties on its “watch list” (key vendors with issues that require monitoring) from 60 to 25. Additionally, Blue Cross NC can better identify persistently underperforming vendors. It has also seen increased executive attention and resources focused on third-party risk and improved experts’ awareness of cross-functional third-party risk issues and priorities.
>
> For more details, see Case Study: Enable Cross-Functional Alignment to Prioritize Third-Party Risks.

FIgure 8: Cross-Functional Third-Party Risk Dashboard Circulated Prior to Monthly Expert Meetings



Cross-Functional Third-Party Risk Dashboard Circulated Prior to Monthly Expert Meetings

Columns provide view across third parties within a silo. **Rows** provide shared view of third parties across silos.

✓ Good ⊖ Cause for Concern ❗ Major Issues

Vendor	Security	Privacy	Audit	Risk	Compliance
Vendor A	⊖	⊖	✓	✓	⊖
July 2022	✓	⊖	✓	⊖	✓
Aug. 2022	⊖	⊖	✓	✓	⊖
Vendor B ▸	⊖	⊖	⊖	✓	⊖
Vendor C ▸	✓	✓	❗	✓	⊖ ?

Month-by-month view highlights trends within relationships and silos.

Detailed view provides context behind ratings.

What does this status mean? Required inputs missing from recertification questionnaire.

Source: Adapted From Blue Cross NC
778074_C

Monitor Forward-Looking Indicators

It is hard to detect enterprise-critical changes in third-party risk before they have an adverse impact. Typical key risk indicators (KRIs) fail to distinguish and prioritize enterprise-level third-party risks. Moreover, these KRIs tend to reflect third-party issues that have already occurred or the organization’s current level of exposure to third-party risk, rather than providing a forward-looking perspective on third-party risk.

Counter this by developing enterprise third-party risk KRIs. To do so, follow this process:

1. **Define enterprise-level third-party risk priorities**. Following the approach described above, begin by defining the aspects of third-party risk that matter most at the enterprise level.

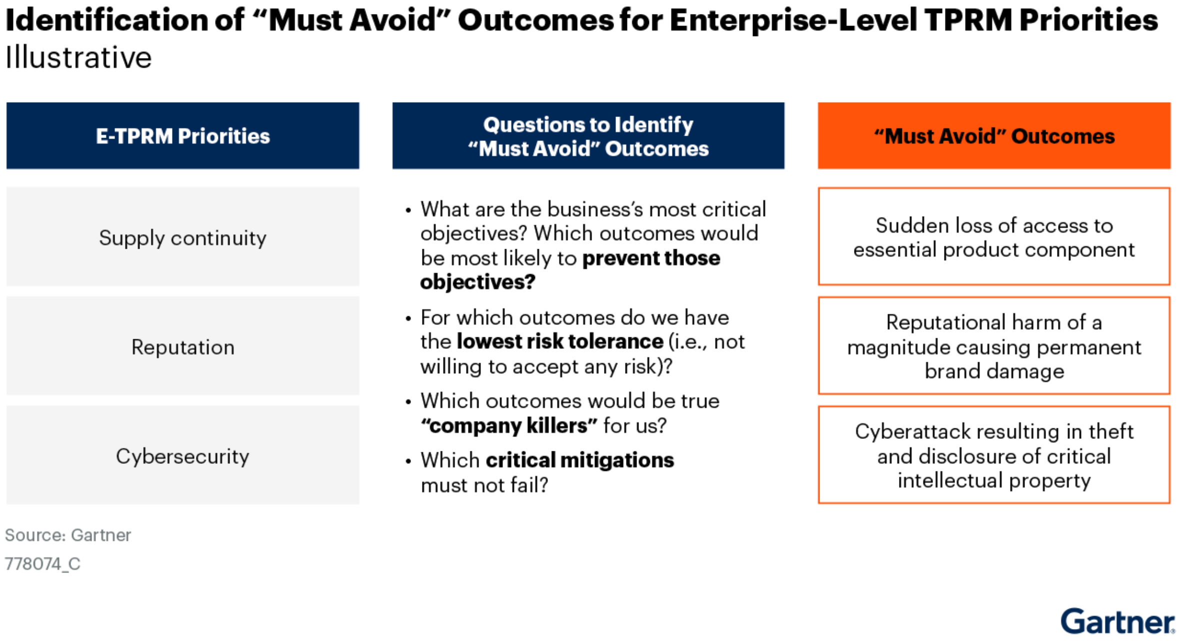
2. **Identify corresponding "must avoid" outcomes.** For each enterprise-critical dimension of third-party risk, identify corresponding severe but preventable third-party outcomes that would prevent achievement of strategic objectives (see Figure 9).

3. **Identify drivers of those outcomes to track.** Perform root cause analysis to identify changes in the world that would make "must avoid" outcomes more likely.

4. **Where possible, leverage existing KRIs.** Review third-party risk KRIs currently tracked by the business and select any that align to the drivers of "must avoid" outcomes you identified.

5. **Identify new E-TPRM KRIs.** Where existing KRIs are insufficient, select new enterprise third-party risk KRIs. Prioritize low-effort monitoring by selecting KRIs that are externally available, objective, benchmarked and scaled.

Figure 9: Identification of "Must Avoid" Outcomes for Enterprise-Level TPRM Priorities



Identification of "Must Avoid" Outcomes for Enterprise-Level TPRM Priorities
Illustrative

E-TPRM Priorities	Questions to Identify "Must Avoid" Outcomes	"Must Avoid" Outcomes
Supply continuity	• What are the business's most critical objectives? Which outcomes would be most likely to **prevent those objectives?** • For which outcomes do we have the **lowest risk tolerance** (i.e., not willing to accept any risk)? • Which outcomes would be true **"company killers"** for us? • Which **critical mitigations** must not fail?	Sudden loss of access to essential product component
Reputation		Reputational harm of a magnitude causing permanent brand damage
Cybersecurity		Cyberattack resulting in theft and disclosure of critical intellectual property

Source: Gartner
778074_C

Conclusion

Heads of ERM must become better at managing third-party risk. They must enhance their ability to maintain and share a concise, prioritized, actionable view of third-party risk at the enterprise level by following our three imperatives. Doing so will significantly increase their organizations' overall effectiveness in managing a unique enterprise risk that is surging in importance.

Recommendations

Heads of ERM devising response strategies for third-party risk should:

- Define enterprise-level priorities by developing a scoring framework based on enterprise-level risk factors to consistently assess the risk posed by individual third parties and prioritize risk actions.
- Enable cross-functional alignment by holding cross-functional discussions of third-party risk that break down functional silos. Use expertise and authority at appropriate moments in the process.
- Monitor forward-looking indicators by devising enterprise third-party risk KRIs, beginning with "must avoid" outcomes. Use root cause analysis to identify potential drivers of the outcomes to monitor.

Presentation Deck

Download presentation slides of this material.

Evidence

[1] **2022 Gartner ERM Survey on Third-Party Risk:** This survey was conducted to benchmark ERM's current role in third-party risk management activities and to test the effectiveness of different ERM approaches at improving ERM's prioritization ability and organization-level third-party risk management outcomes. It was conducted online during July and August 2022 among 74 risk leader respondents representing a diverse range of industries, geographic locations and revenue bands. Respondents were screened to include only current heads of ERM and key deputies.

[2] **2022 Gartner Risk Committee Survey:** This survey was conducted to assess executive risk committees' perspective on third-party risk management, ERM's current role and effectiveness, and opportunities for improvement. It was conducted online during July and August 2022 among 100 executive risk committee members representing a diverse range of industries, geographic locations and revenue bands. Respondents were screened to include only current executive risk committee members with oversight of third-party risk.

Recommended by the Authors

Case Study: Rate Third Parties at the Enterprise Level for Risk-Based Prioritization

Case Study: Enable Cross-Functional Alignment to Prioritize Third-Party Risks

Find Third-Party Risk Indicators That Matter — Here's How

Common Gaps in Third-Party Risk Management

Tool: Third-Party-Risk Taxonomy

Risk in Financial Services: The Changing Role of ERM in Third-Party Risk Management

ERM Risk Response Accelerator for Supply Chain Risk: Topic Guide

Case Study: Risk Appetite and Tolerance-Focused Strategic Risk Reporting (Cenitex)

Disclaimer: The organization (or organizations) profiled in this research is (or are) provided for illustrative purposes only, and does (or do) not constitute an exhaustive list of examples in this field nor an endorsement by Gartner of the organization or its offerings.

Table 1: Typical ERM Roles Versus Characteristics of Third-Party Risk

Typical ERM Role	Characteristic of Third-Party Risk That Makes ERM Role Less Effective
Aggregator: Combines inputs from across the business to determine what's most important	Many heterogeneous risks that vary greatly in importance across the business are combined.
Thought Partner: Spends time with risk owners to identify key issues and test what matters most to them	Risk ownership is naturally distributed among many different people/functions.
Trend Spotter: Uses subject matter expert perspective or data to anticipate emerging issues in the risk landscape	Issues are too numerous and diverse; available data is point-in-time and lagged.

Source: Gartner

Table 2: The Three Imperatives of E-TPRM for Heads of ERM

Imperative for ERM	What It Means	Why It Works
Define enterprise-level priorities	Isolate and combine **only those inputs that matter most** at the enterprise level.	With an explicit, shared set of priorities, ERM can aggregate the inputs that matter most to the enterprise.
Enable cross-functional alignment	Help risk co-owners **obtain a holistic view** and create opportunities for them to work toward **consensus.**	By facilitating thought partnership among risk co-owners, ERM uses diverse expertise and aligns action.
Monitor forward-looking indicators	**Limit focus** to the most critical emerging issues and **track** them.	A focused set of easily monitored indicators enables ERM to reliably spot enterprise-critical trends.

Source: Gartner