Gartner

Third-Party Risk Management Benchmarking Report 2023

This is a best-practice benchmarking report from our 2022 Gartner Cross-Functional Third-Party Risk Management Survey. Legal and compliance leaders can learn key trends across functions regarding the state of the third-party network, TPRM governance, due diligence and monitoring.

Overview

Key Findings

- Third-party networks continue to expand, with third-party startups and business model innovators increasingly having a role in the organization's extended enterprise. This results in increased targeted oversight from the board and senior leaders.
- A majority of organizations have implemented centralized or federated models of third-party risk management (TPRM) governance, representing a marked shift from our 2019 results where a majority adhered to functional or distributed models. This shift should help desilo critical third-party risk information.
- Although many organizations use exhaustive due diligence practices, nearly half are 0% to 50% confident in the information third parties provided in their due diligence questionnaires.
- With many lacking confidence in self-reported third-party information, organizations are more likely to employ resource-intensive in-house monitoring strategies.

Strategic Planning Assumption

By 2025, legal and compliance oversight of environmental, social and governance (ESG) strategy and disclosures will drive new investments in TPRM solutions at 50% of organizations.

Survey Objective

In 2022, we conducted a cross-functional TPRM survey of 12 functions to ascertain the changing nature of third-party networks and the impact of a broad range of TPRM activities and subjects, including governance, due diligence and monitoring. A similar survey was conducted in 2019 on the same topics, which surveyed an audience of 11 functions.

Data Insights

Introduction

Third-party networks continue to expand, with third-party startups and business model innovators increasingly joining these networks. The greater presence of high risk in networks is likely prompting boards and senior leaders to increase and better target oversight of their TPRM programs.

Many organizations are also implementing governance strategies to improve information sharing across functions. In some cases, they are implementing centralized or federated models of TPRM governance. For many others, centralized TPRM functions that lead key aspects of the program have emerged.

Even with increased information sharing across functions and TPRM program centralization, many organizations do not trust the quality of information from third parties. Many are still using resource-intensive due diligence practices to gather as much information as possible. However, these practices are yielding poor quality information — almost half of leaders are 0% to 50% confident in the information provided — which limits their usefulness. Because of this lack of confidence, organizations are relying on resource-intensive in-house monitoring strategies.

As a result, many are limiting recertifications of third parties to one to three years, instead of more often than annually. Others are implementing mechanisms to flag third parties for recertification rather than having a set schedule for recertifications.

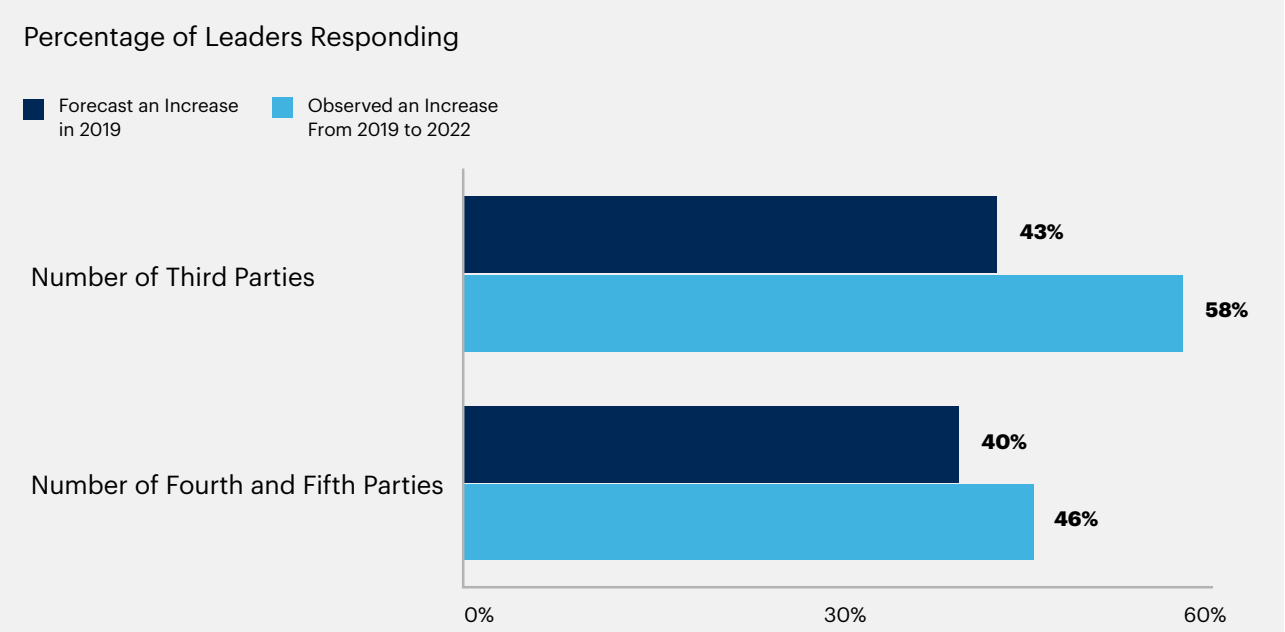
State of the Third-Party Network

Third-party networks continue to expand, with third-party startups and business model innovators increasingly joining these networks. These new higher-risk additions to the networks are prompting boards and senior leaders to increase scrutiny and better target oversight of their TPRM programs.

Increased Oversight of More Third, Fourth and Fifth Parties

Fifty-eight percent of respondents observed an increase in the number of third parties (see Figure 1). This is a 15 percentage point increase from 2019 projections. Additionally, 46% observed an increase in the number of fourth and fifth parties, a 6 percentage point increase from 2019 projections. Forecasting data from 2022 indicates that about half of all respondents are anticipating even more increases in the number of third parties (52% indicating so) and fourth and fifth parties (48% indicating so).

Figure 1: Observed Changes Within the Third-Party Network From 2019 to 2022 Compared to 2019 Forecasts

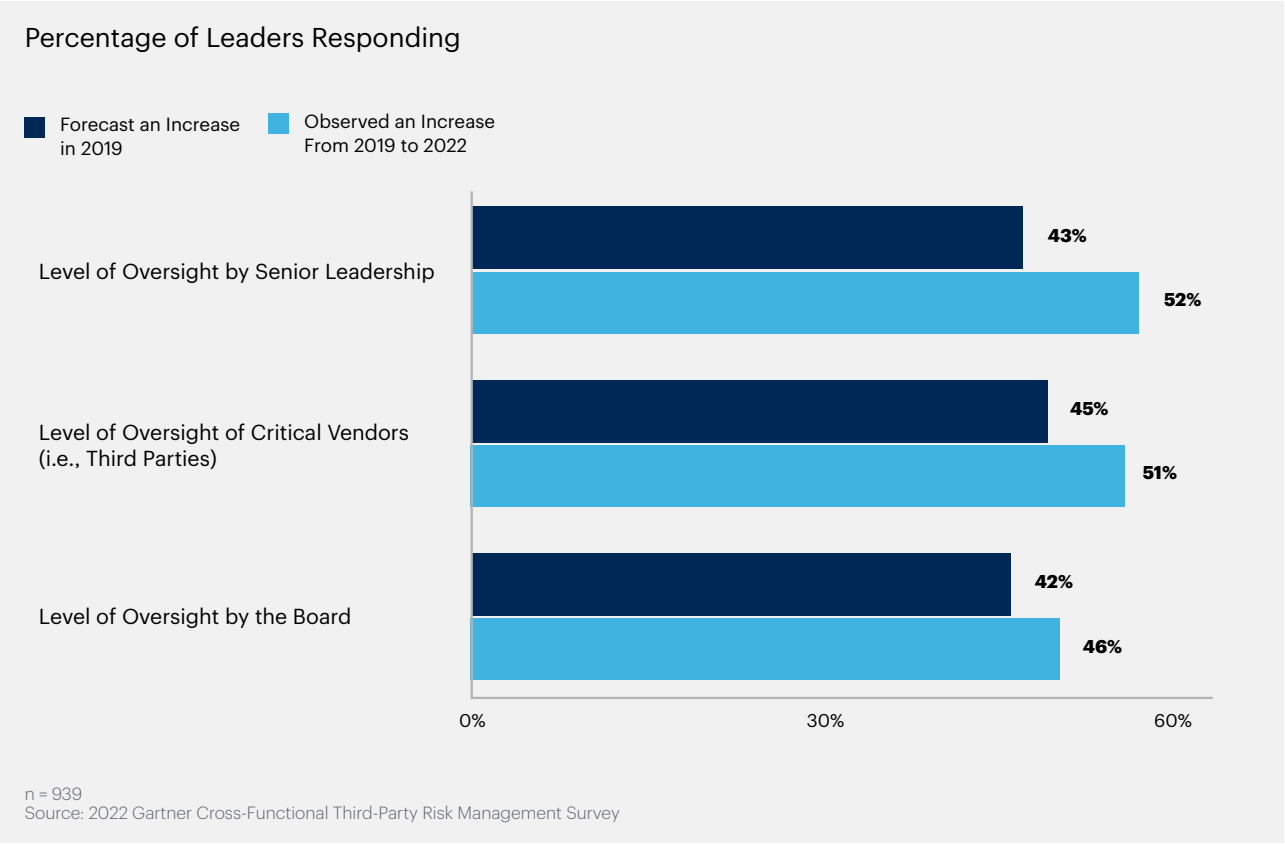


n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner®

Forty-two percent of respondents believe third parties are more critical for their organization's profitability than they were just three years ago. With such widespread belief, many organizations are increasing oversight of their TPRM program. Over half of respondents (51%) observed an increase in oversight on critical vendors in the last three years, a 6 percentage point increase over 2019 projections. In addition, more than 50% observed an increase in senior leader oversight of the network, while 46% indicated an increase in board oversight (see Figure 2).

Figure 2: Observed Changes in Oversight of Third-Party Networks From 2019 to 2022 Compared to 2019 Forecasts



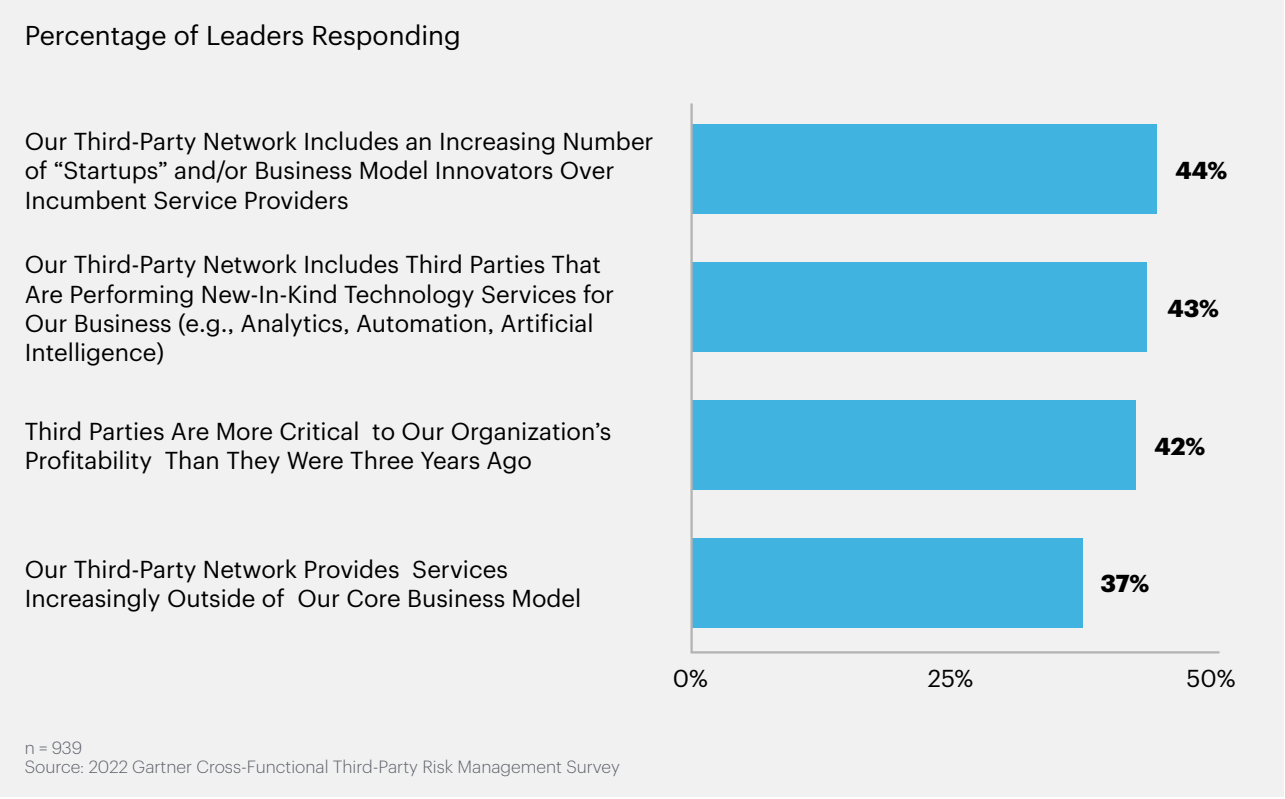
n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner®

More Organizations Include Startups and Business Model Innovators in Their Third-Party Networks

Many of the new third, fourth and fifth parties differ from the traditional third parties organizations have used before. Indeed, 44% responded that startups or business model innovators increasingly comprise their third-party networks (see Figure 3). Additionally, 43% noted an increasing number of their third parties are performing new-in-kind technology services for their business. Another 37% noted an increasing number of third parties performing services outside of their organization's core business model.

Figure 3: Level of Agreement on the Nature of Third-Party Networks



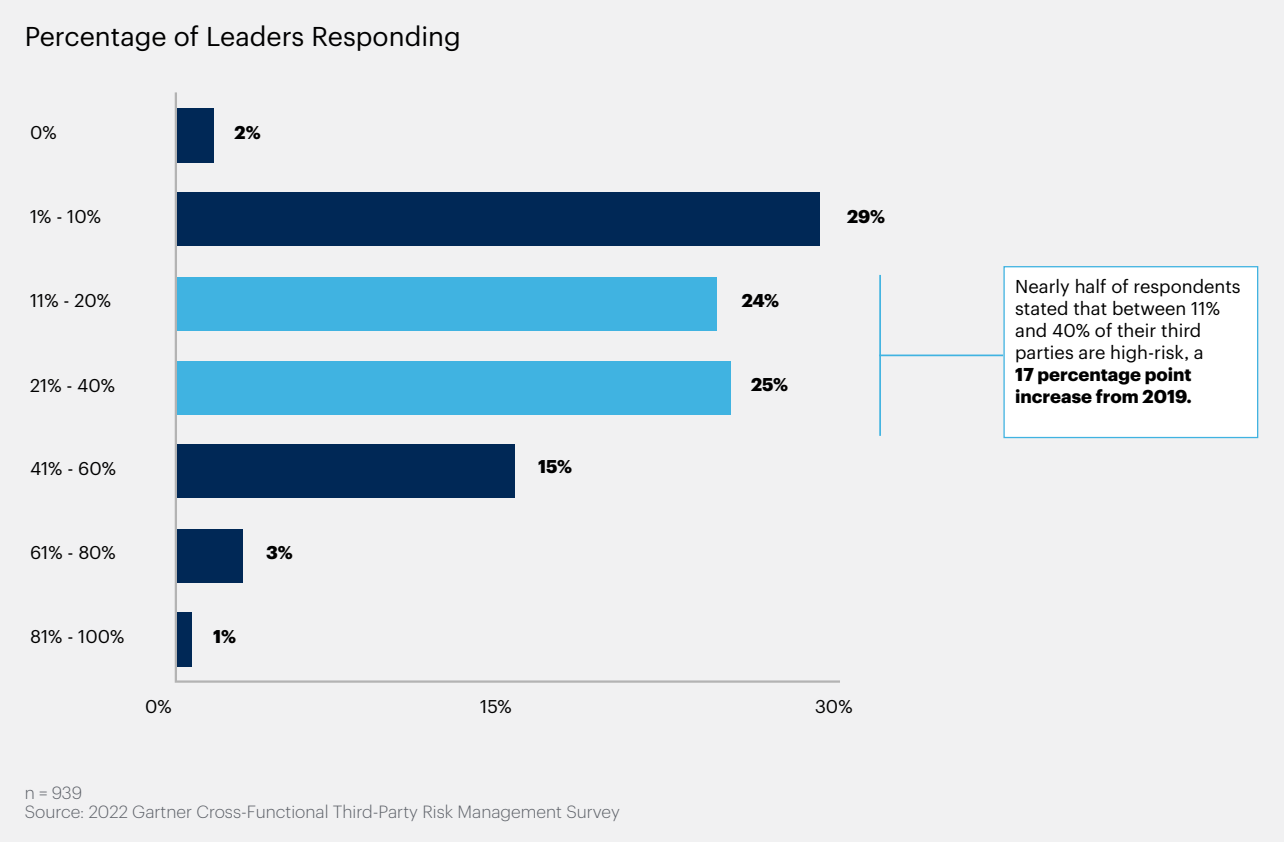
n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner

Organizations Increasingly Working With High-Risk Third Parties, Prompting More Targeted Oversight

With more alternative third parties in addition to increased oversight, organizations are increasingly working with high-risk third parties. Nearly half of respondents state that between 11% and 40% of their third parties are high-risk, a 17 percentage point increase from 2019 (see Figure 4).

Figure 4: Percentage of High-Risk Third Parties in Third-Party Network



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

The increased number of third, fourth and fifth parties, oversight of third-party networks and the number of high-risk third parties are pushing leaders to be judicious in resourcing third parties for effective risk management. To best triage their resourcing, organizations should focus their efforts on high-risk third parties, even while the volume continues to increase.

Gartner®

Governance

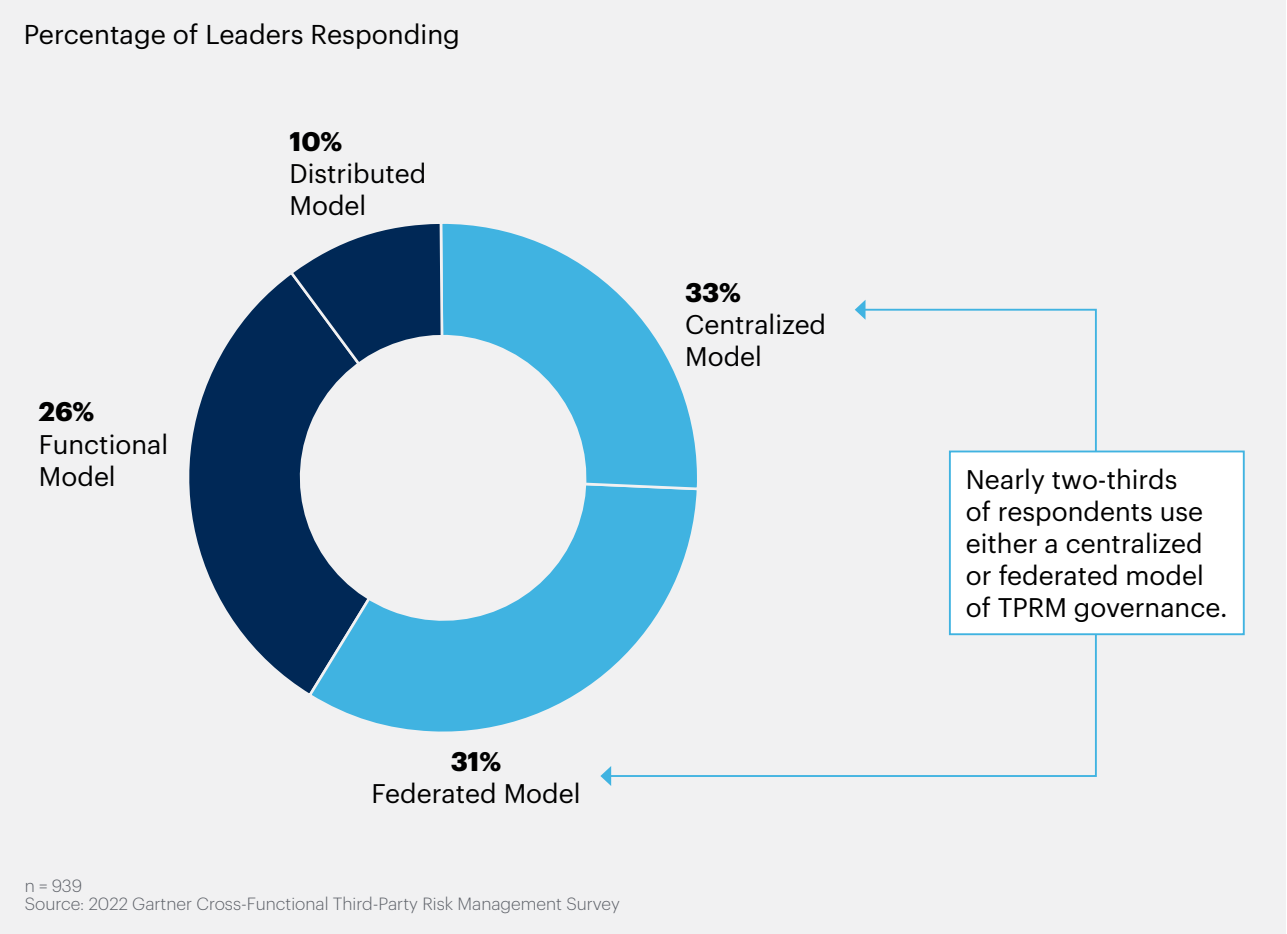
As organizations are increasingly targeting TPRM program oversight, many are implementing governance strategies to improve information sharing across functions. In 64% of cases, organizations are implementing centralized or federated models of TPRM governance. For many others, centralized TPRM functions that lead key aspects of the program have emerged.

Increased Implementation of Centralized or Federated Models of TPRM Governance

Organizations generally organize their TPRM program around four main models of governance: centralized, federated, distributed and functional models. Centralized and federated models focus on creating a more effective information-sharing system within the organization by desiloing critical third-party risk information. While the centralized model is primarily managed by a single function, federated models typically include multiple functions, and a single cross-functional group makes final decisions. On the other hand, both distributed and functional models have little enterprise-level visibility (i.e., little information sharing between functions) compared to the centralized and federated models.

In the past three years, organizations have shifted from distributed or functional models to centralized or federated TPRM governance models. In 2019, 60% of respondents used either a distributed or functional model, while 39% used either a centralized or federated model. But now, 64% of respondents use either a centralized or federated model of TPRM governance, a 25 percentage point increase from 2019. Additionally, 36% of respondents use either a distributed or functional model, a 26 percentage point decrease from 2019 (see Figure 5).

Figure 5: Governance Model Used for TPRM Efforts



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

These results suggest that as organizations target their TPRM efforts on high-risk third parties, many are pivoting to desiloing critical third-party risk information. Many are doing this by moving toward centralized or federated models.

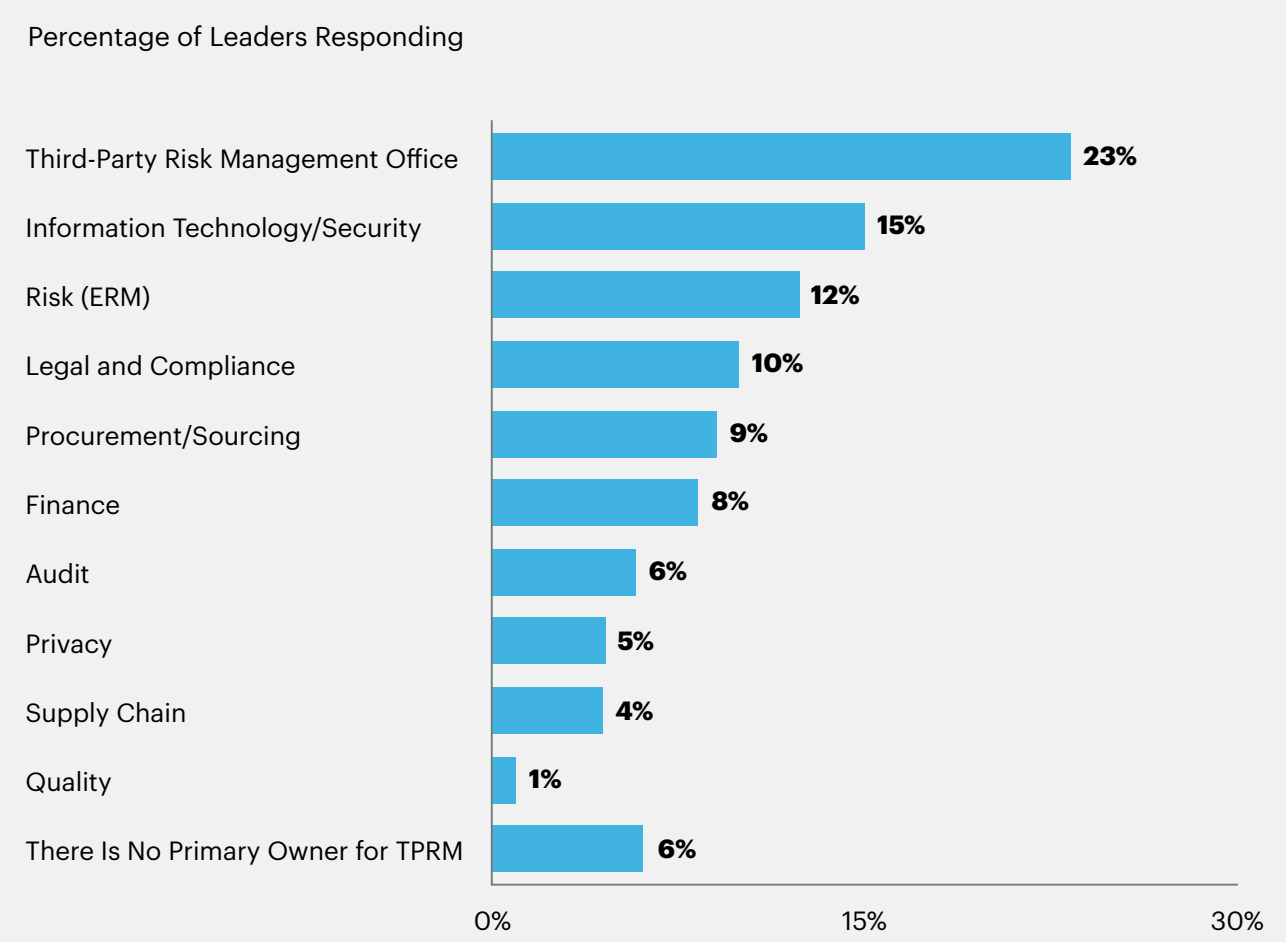
Despite a majority implementing federated or centralized models of TPRM governance to desilo information, key TPRM information remains siloed between functions. While 51% of respondents agree their function typically shares information related to TPRM in a timely manner, only 44% agree they can always integrate the information shared by other functions in their risk analysis system. Additionally, less than half agree their software systems and technology tools make it easy to share information on TPRM.

Gartner

TPRM Function Emerges as Top Functional Owner, and Audit Allocates Greatest Budget to TPRM

With increased information sharing across functions, organizations are increasingly having centralized TPRM office functions handle key aspects of the program. In fact, 23% of leaders indicated that the TPRM office is the primary functional owner of TPRM in their organization (see Figure 6).

Figure 6: Functional Owners of TPRM



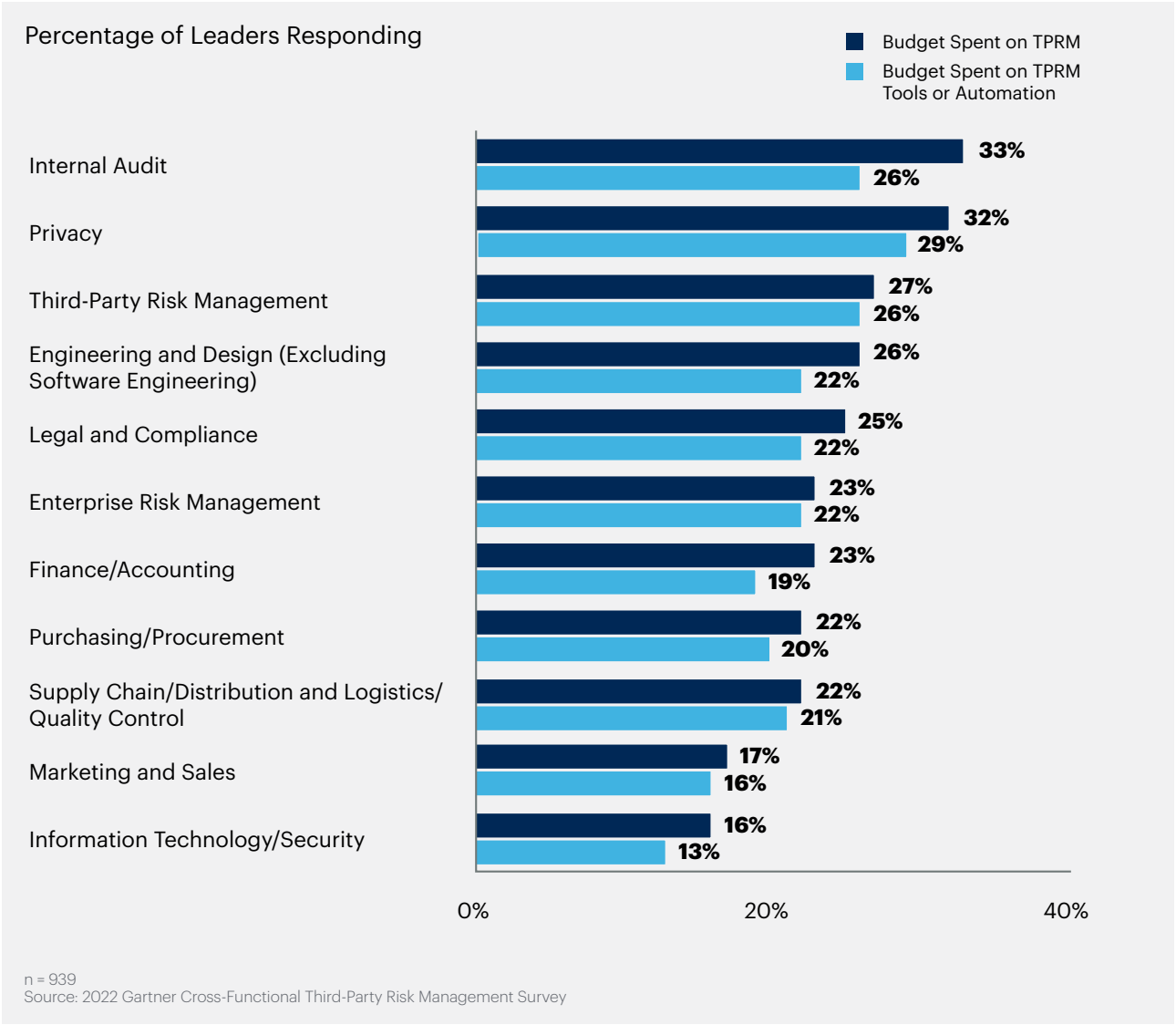
n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner®

Centralized TPRM offices have grown more common in recent years as organizations increasingly rely on the centralized or federated models of TPRM governance. EY found that from 2019 to 2020, organizations with centralized TPRM functions increased from 50% to 60%. [1,2,3] Following the TPRM office, information technology/security (15%) and risk (12%) emerged as the second and third functional owners of TPRM, respectively, with the legal and compliance functions coming in as fourth at 10%.

Although the TPRM office is the primary owner of TPRM for many organizations, internal audit has the largest average percentage of its budget being spent on TPRM in general (see Figure 7). Additionally, audit is also a top spender on TPRM tools or automation, with an average of 26% of its budget being spent on it. Audit's high percentages may be partly due to the traditionally high costs of audits, which audit primarily owns as a TPRM activity. Almost a third of respondents indicated audit is primarily responsible for conducting third-party audits.

Figure 7: Percentage of Functional Budget Spent on TPRM and TPRM Tools or Automation in the Last Fiscal Year



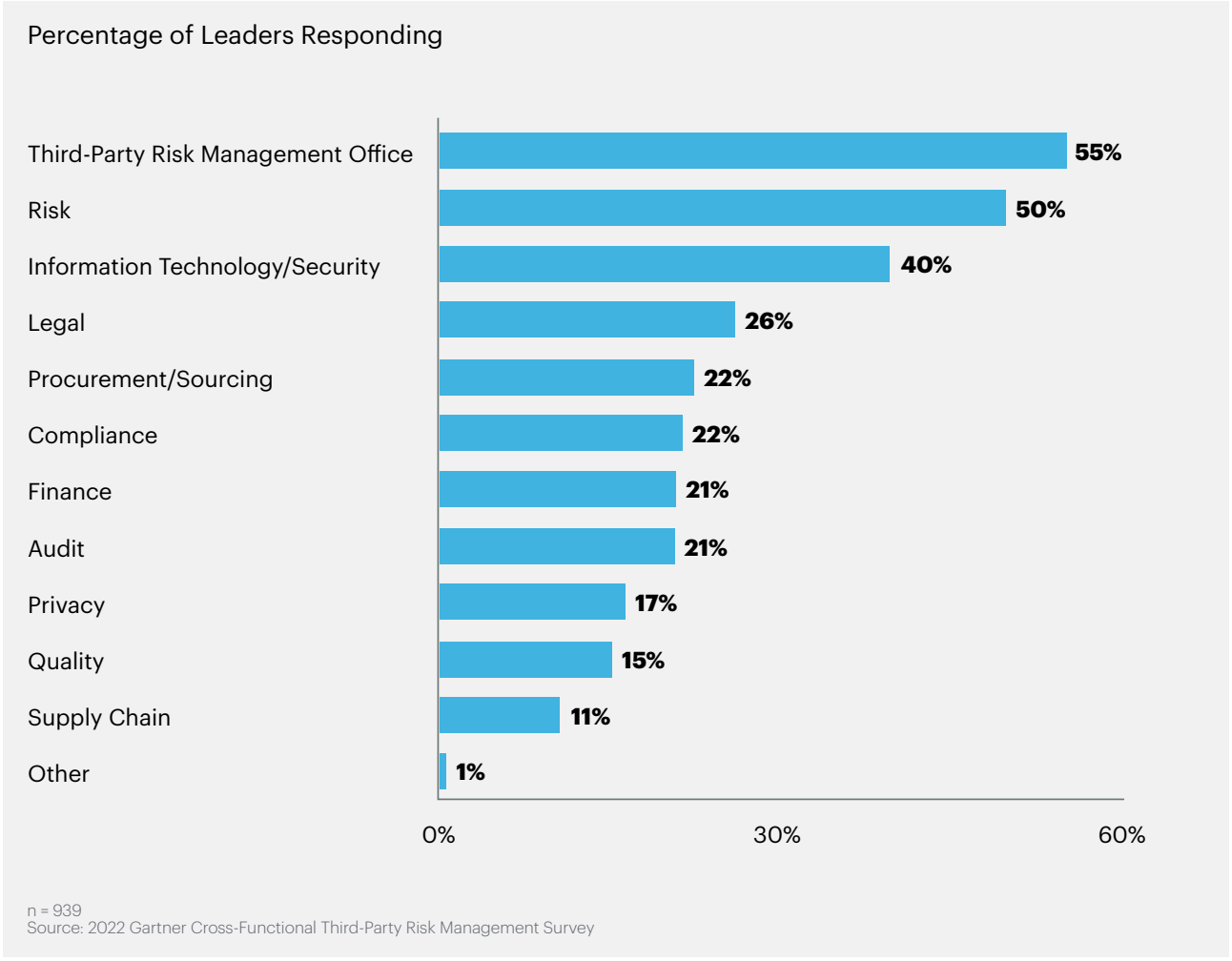
n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner

Privacy and TPRM are also top budget spenders, with an average 32% and 27% of their budget being spent on TPRM in general, respectively. Legal and compliance functions were fifth for the average percentage of their budget spent on TPRM in general, with budget spent on tools and automation being 25% and 22%, respectively.

Although the TPRM office is not the top spender on TPRM, many organizations rely on the function to lead aspects of their TPRM program. More than half of respondents collaborate most often with the TPRM office (see Figure 8).

Figure 8: Top Functions Respondents Collaborate With on TPRM Activities



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner®

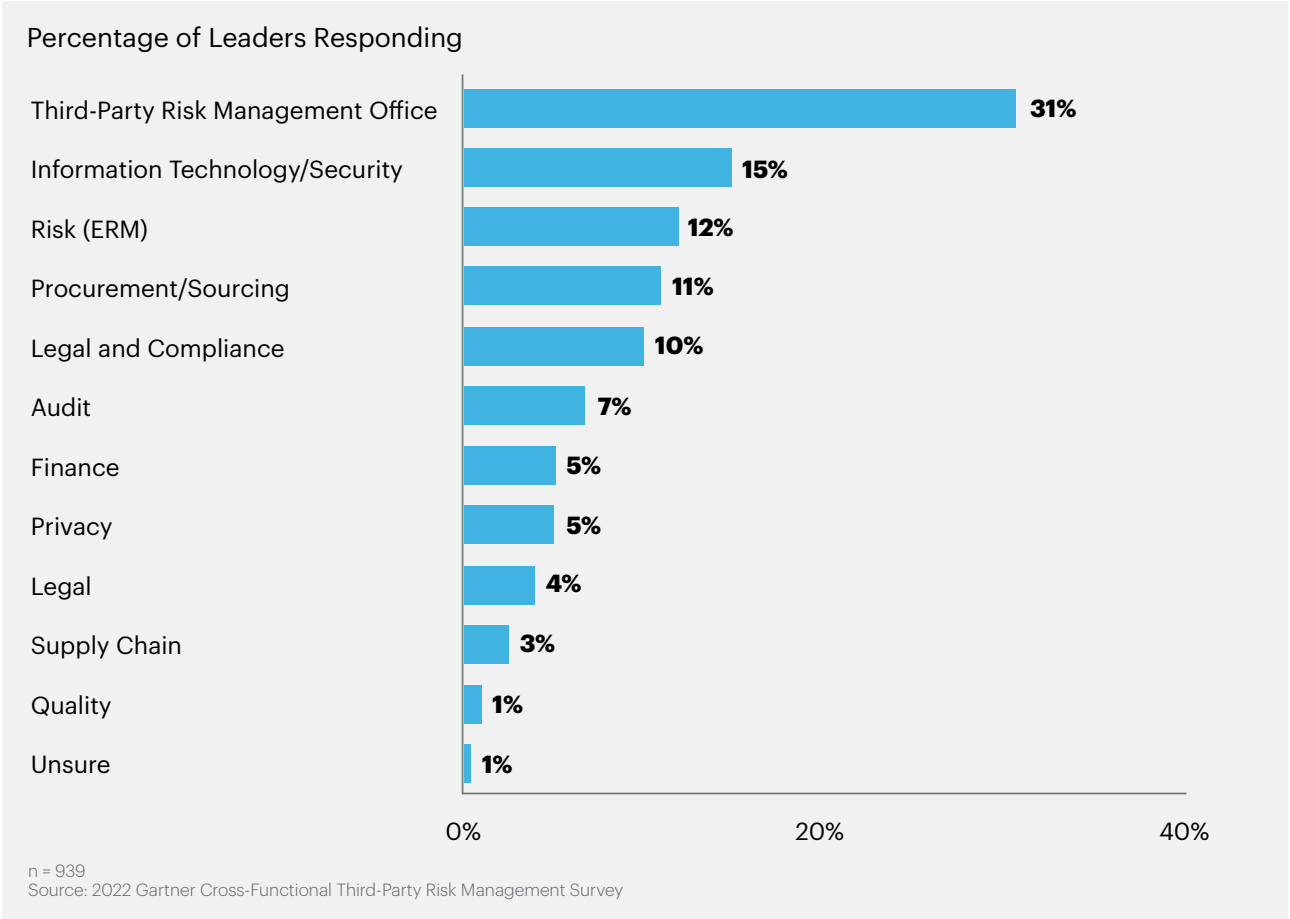
The TPRM office, information technology/security and legal functions have the most prevalent interfunctional coordination. However, less than a quarter of respondents say they most coordinate with other functions, including:

- Audit
- Compliance
- Finance
- Privacy
- Procurement/sourcing
- Quality
- Supply Chain

These results suggest that TPRM activities and processes are still siloed between many functions, leading to a loss of information. Despite organizations' ongoing concerns over privacy risks — half anticipate increased scrutiny of third parties' privacy controls in the next three years — privacy remains a largely siloed function. Only 17% of respondents chose privacy as a top collaborating function.

Additionally, functional ownership of reporting TPRM activities to the board is in line with other findings, indicating the TPRM office taking a leading role (see Figure 9).

Figure 9: Functional Ownership of Reporting TPRM Activities to the Board



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

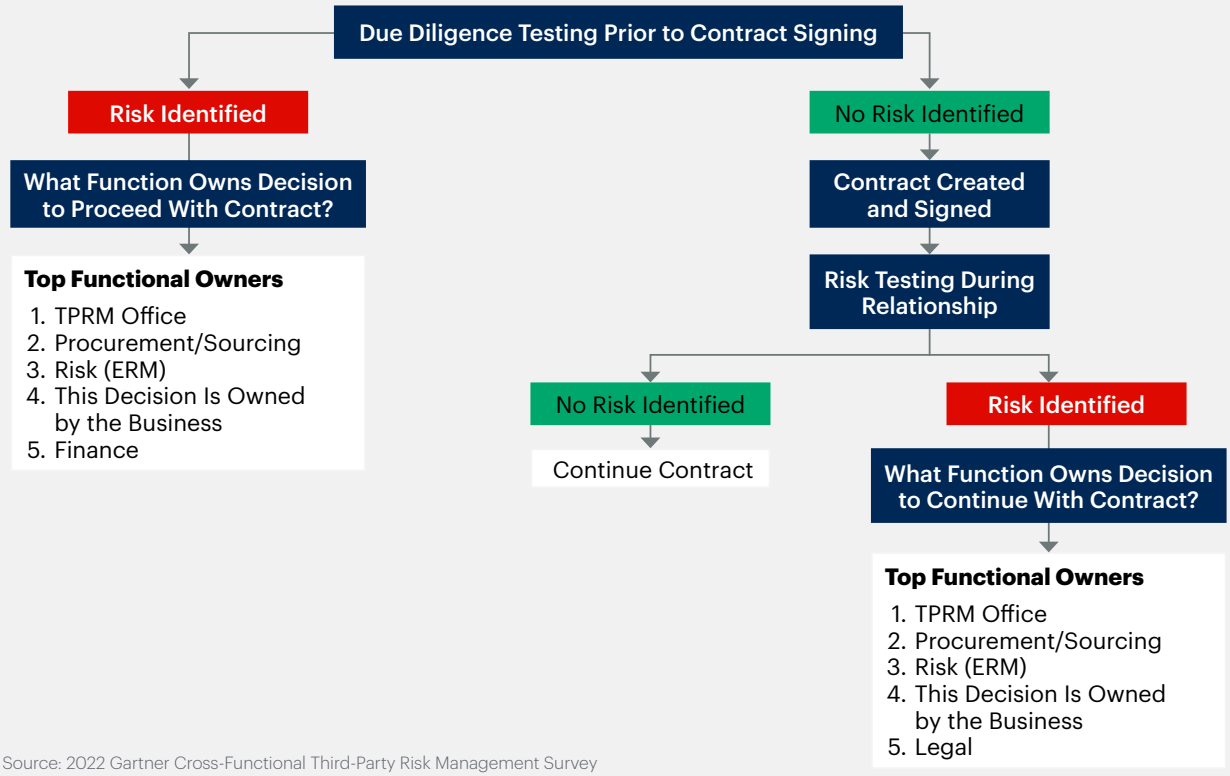
Gartner

About a third of respondents (31%) listed the TPRM office as the top functional owner of reporting TPRM activities to the board. Information technology/security and risk were the top second and third functional owners for reporting, with 15% and 12% of respondents indicating so, respectively.

TPRM Office Function Is the Top Owner of Decision to Proceed With or Continue Third- Party Relationships

Overall, the number of rejections of third parties in 2022 increased slightly. The most pronounced change was 41% of respondents indicating their organization rejects 11% to 25% of deals, an increase of 15 percentage points from 2019 to 2022. Functional ownership of the decision on whether to proceed with or continue third-party relationships is fragmented across different functions. However, the TPRM office remains the leading function to own said decisions (see Figure 10).

Figure 10: Decision Ownership of Proceeding With or Continuing Third-Party Relationships After Risk Identified



Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner

If a risk is identified during due diligence testing prior to contract signing, a quarter of respondents indicated that the TPRM office would own said decision. After creating a third-party relationship, if a risk is identified during the relationship, the functional ownership of the decision to continue is fairly consistent with ownership prior to contract signing.

Due Diligence

Even with increased information sharing across functions and TPRM program centralization, many organizations are still using resource-intensive due diligence practices to gather as much information as possible. However, these practices are yielding poor quality information, leading to growing distrust of information quality from third parties.

Due Diligence Is Resource-Intensive, Yet Yields Poor Quality Information

Nearly half of respondents believe it is important to identify all possible risks during due diligence to learn everything they can about a third party's risk profile before moving forward with the engagement (see Table 1). To achieve this goal, 47% have added more questions to their function's third-party due diligence questionnaire. These activities and beliefs can be defined as exhaustive due diligence activities (i.e., those that focus on gathering information across many different risk categories).

Table 1: Due Diligence Activities

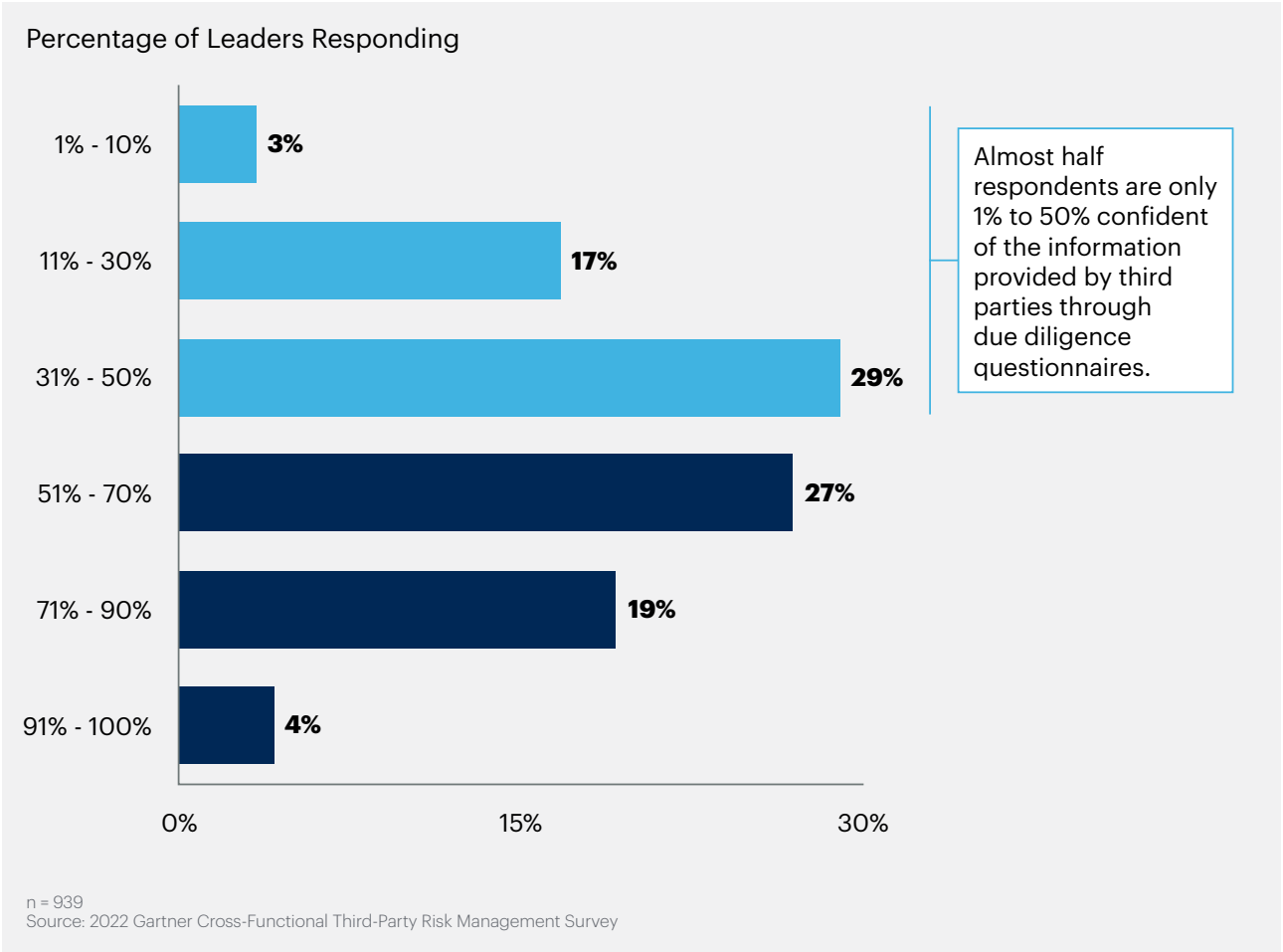
Exhaustive Activities **Those that focus on gathering information across many risk categories**	**Streamlined Activities** **Those that focus on the most critical risks**
47% of leaders believe it is important to identify all possible risks to learn everything they can about a third party's risk profile before moving forward.	47% of leaders believe it is important to use a single due diligence questionnaire (that incorporates input from relevant functions) during the screening process before onboarding.
47% of leaders have added more questions to their function's third-party due diligence questionnaire.	42% of leaders believe it is important to administer a due diligence questionnaire to new third parties that targets only the most critical risks.

n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Despite so many organizations using exhaustive due diligence practices and nearly half of respondents adding more questions to their due diligence questionnaires, many are still not retrieving good quality information (i.e., complete and sufficient data).

Nearly half of respondents are 1% to 50% confident of the information provided by third parties through due diligence questionnaires (see Figure 11). Even more concerning is that less than 5% of respondents are 91% to 100% confident of the information provided in due diligence questionnaires. In addition, over a quarter answered that 51% or more of the information initially received from third parties from the questionnaires is incomplete and or offered insufficient information.

Figure 11: Confidence Level of Information Provided by Third Parties Through Due Diligence Questionnaires



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Organizations aligning with exhaustive activities can save both time and resources and potentially improve information quality. By shifting to more streamlined due diligence activities, organizations can target the most critical risks and questionnaires that ask the right questions. Our Ignition Guide to Conducting Due Diligence will help leaders assess the critical business risks presented by their third-party network and build a more effective due diligence strategy.

Gartner®

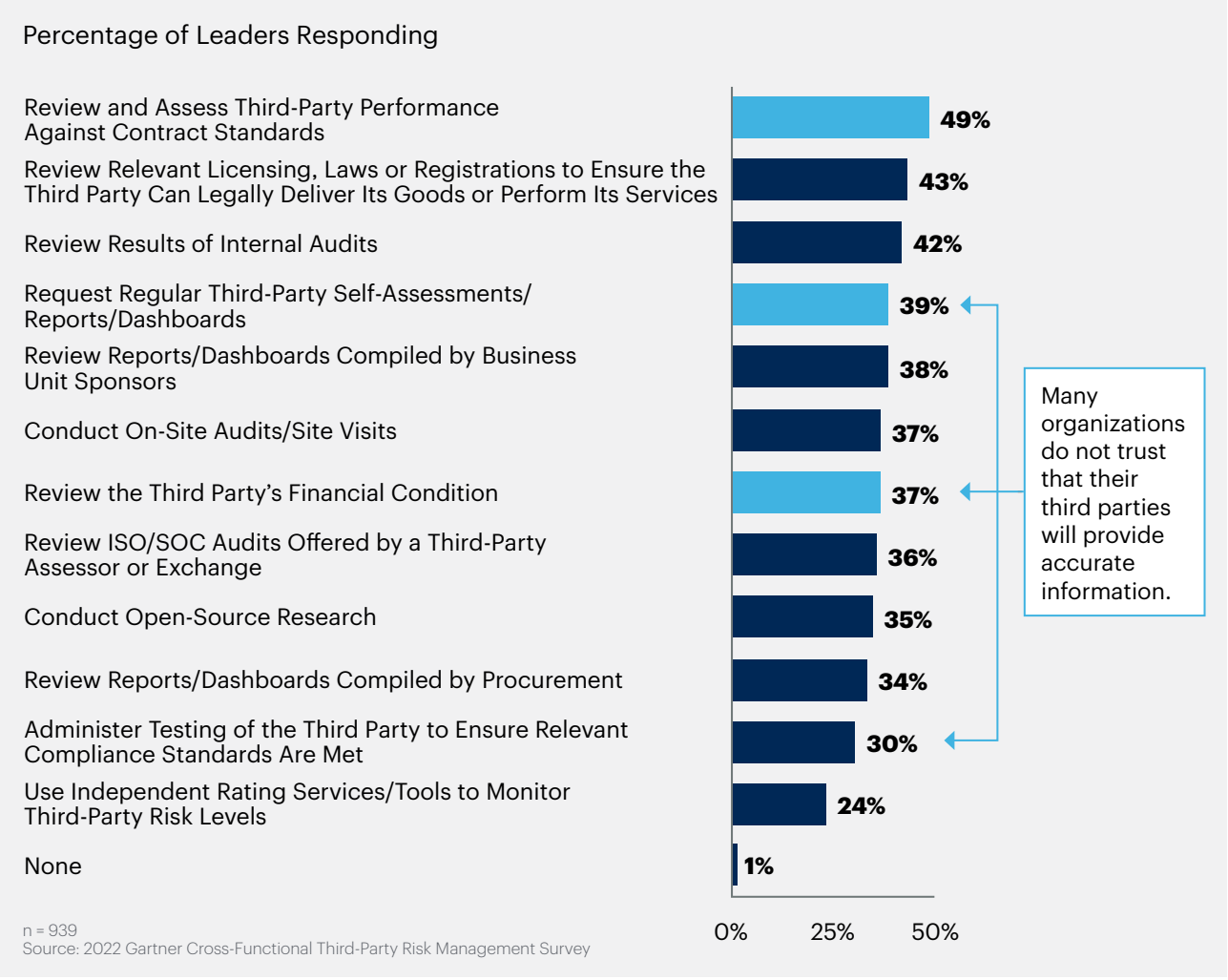
Monitoring

With many lacking confidence in the quality of self-reported third-party information, organizations are relying on resource-intensive in-house monitoring strategies. As a result, many are limiting recertifications of third parties to one to three years, instead of more than annually. Others are implementing mechanisms to flag third parties for recertification, rather than having a set schedule for recertifications.

Organizations Decrease Employment of Third-Party Self-Reporting Monitoring Strategies

Many organizations are unlikely to employ third-party self-reporting monitoring strategies as they have had experience in gaining poor quality data from third parties through due diligence activities (see Figure 12). Only 30% of respondents actually administer third-party testing to ensure relevant compliance standards are met, a 14 percentage point decrease from 2019. In addition, only 37% review their third parties' financial conditions. Lastly, only 39% request regular third-party self-assessments, reports and/or dashboards, nearly a 10 percentage point decrease from 2019.

Figure 12: Employment of Monitoring Strategies for Third Parties



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

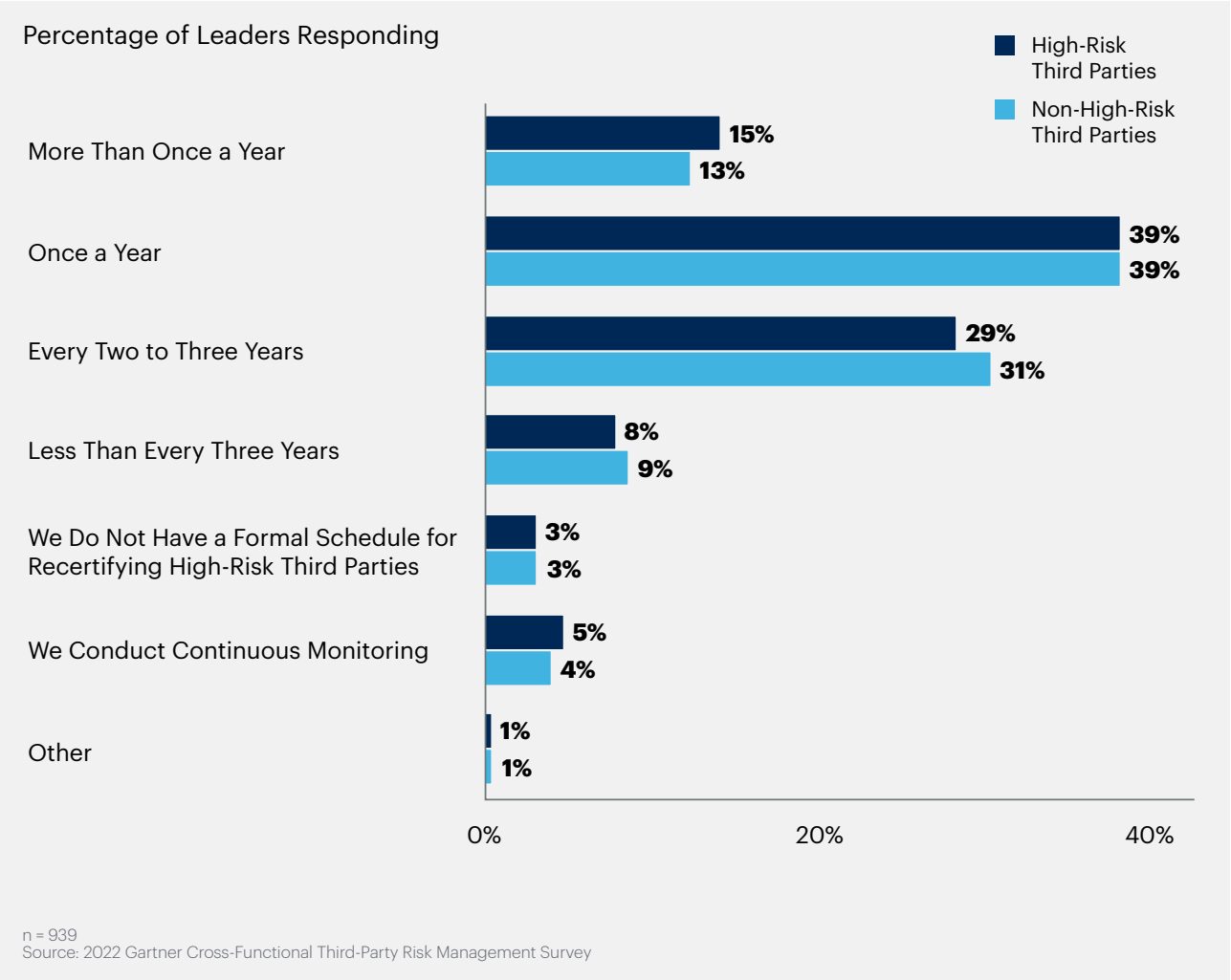
Gartner

As organizations decrease usage of third-party self-reporting monitoring strategies, they are instead overresourcing in-house monitoring strategies. This is potentially increasing employee burden. Nearly half of respondents review and assess third-party performance against contract standards. In addition, 43% review relevant licensing, laws or registrations to ensure the third party can legally deliver its goods or perform its services.

Organizations Are More Likely to Recertify High-Risk Third Parties Every One to Three Years, Rather Than More Than Annually

Nearly 40% of leaders recertify high-risk third parties once a year. This is more than a 10 percentage point reduction from 2019, when 51% of leaders recertified high-risk third parties annually (see Figure 13). The rates of recertifications done more than annually also reduced by more than 10 percentage points. In 2019, more than a quarter recertified high-risk third parties more than annually, while only 15% did so in 2022.

Figure 13: Recertification Rates for Third Parties



n = 939
Source: 2022 Gartner Cross-Functional Third-Party Risk Management Survey

Gartner

Overall, leaders are now more likely to recertify high-risk third parties every one to three years. In fact, nearly a third recertify high-risk third parties every two to three years. This is a shift from 2019, when a majority of leaders would recertify high-risk third parties either more than once a year or annually. This suggests that organizations' overresourcing of in-house monitoring strategies has caused some organizations to limit their recertification efforts. These organizations may not have the resources to conduct as many recertifications as they might prefer.

Additionally, organizations are increasingly implementing mechanisms to flag third parties for recertification and review, rather than having a set schedule for recertifications. Half of respondents agree their function has mechanisms (e.g., information channels, systems, processes) in place to learn about changes in the scope or purpose of third- party relationships. Also, 63% of respondents recertify third parties after receiving external information about a third party. And 70% or more of the time, they review that third party to identify possible new risks (outside the scope of what was identified previously).

Conclusion

Our research demonstrates that third-party networks continue to expand, with third-party startups and business model innovators increasingly joining these networks. The greater presence of high risk in networks is likely prompting boards and senior leaders to increase and better target oversight of the TPRM program. As organizations increase and better target TPRM program oversight, many are implementing governance strategies to improve information sharing across functions. Even with these efforts, many are using resource-intensive due diligence practices to gather as much information as possible. However, these practices are yielding poor quality information, limiting their usefulness. Because of this lack of confidence, organizations are increasingly relying on resource-intensive inhouse monitoring strategies. As a result, many are limiting recertifications of third parties to one to three years, instead of more than annually. Others are implementing mechanisms to flag third parties for recertification, rather than having a set schedule for recertifications.

Evidence

The 2022 Gartner Cross-Functional Third-Party Risk Management Survey analyzed 12 functions to inform the third-party risk management insights in this report. The data presented reflects the answers of respondents who attest their organizations successfully identify and remediate third-party risk. The surveyed functions were compliance, engineering and design (excluding software engineering), enterprise risk management, finance and accounting, information technology and security, internal audit, legal, marketing and sales, privacy, purchasing and procurement, supply chain/distribution and logistics, and dedicated third-party risk management functions or offices.

[1] How Can Finite Resources Tackle an Infinite Risk Universe?, EY.

[2] How Businesses Can Address a Growing Range of Third-Party Risks, EY.

[3] Organizations surveyed were in sectors such as retail, banking, insurance, manufacturing, technology, media and entertainment, utilities and health.

Gartner®

Actionable, objective insight

Position your legal organization for success. Explore these additional complimentary resources and tools:

Report

Legal and Compliance Risk Management Framework

Mitigate legal and compliance risk with Gartner insights.

Download Report

Report

Third-Party Risk Management Governance and Technology Investments

Understand top insights and trends for third-party risk management (TPRM).

Download Report

eBook

Third-Party Risk Management (TPRM)

Shift from a point-in-time to an iterative approach to manage new third-party risks.

Download eBook

Webinar

Manage Risks to Profitability in Third-Party Networks

Hear the latest Gartner benchmarking and best practices on third-party risk management.

Watch Now

Already a client?
Get access to even more resources in your client portal. Log In

Gartner

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/legal-compliance

Stay connected to the latest insights

Gartner®