Gartner for Legal, Risk & Compliance

Third-Party Risk Management Governance and Technology Investments: A Gartner Trend Insight Report

By Ipshita Soni, Koray Kose, Nicholas Sworek

Gartner

Third-Party Risk Management Governance and Technology Investments: A Gartner Trend Insight Report

Published 10 February 2022 - ID G00763018 - 16 min read

By Analyst(s): Ipshita Soni, Koray Kose, Nicholas Sworek

Initiatives: Compliance Program Management; Procurement Management; Sourcing and Procurement

The disruptions caused by the pandemic have pushed organizations to look for more effective approaches to managing third-party risks. Chief compliance and ethics officers should use this research to understand top insights and trends in TPRM to support efforts in this area.

Overview

Opportunities and Challenges

- While 44% of organizations said COVID-19 was the most significant disruptive event in the past two years, only 50% of organizations indicated their crisis management/business continuity capabilities were effective during their most disruptive event, such as the COVID-19 pandemic.
- Organizations are in a poor position to manage critical third-party risks. Only 28% of organizations continuously monitor third parties throughout engagement cycles, and just 16% of organizations say they effectively manage third-party risks.
- The push for improved environmental, social and governance (ESG) initiatives has created a renewed focus on third-party risk management (TPRM) activities and application investments. This focus is pressuring organizations to rethink their due diligence requirements to encompass ESG-related criteria and perform greater scrutiny of third-party practices and nth parties.

What You Need to Know

- Fifty-eight percent of supply chain organizations have increased their technology budgets to manage critical supply chain risks, as demonstrated in our 2021 Gartner Supply Chain Risk and Resilience Survey. Our survey further indicates investments in risk management and compliance are projected to increase by 30% for 2022.
- Over 29% of TPRM vendors are enhancing their solutions in response to the global momentum for ESG by currently supporting ESG-related third-party risks. Others are looking to enhance their solutions by including support for ESG, given the rapid growth of related regulations.
- Given the increased stakeholder oversight of TPRM initiatives, organizations are pushing for increased accountability for TPRM activities and are requiring a coordinated, consolidated view into TPRM. This goal can be achieved by implementing TPRM governance that clarifies ownership of activities within TPRM and oversees them to ensure effective mitigation of risks.

Strategic Planning Assumption

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

Insight From the Experts

Single Primary Owner of TPRM Will Be Needed to Improve Accountability

The disruptions caused by the COVID-19 pandemic have proved to organizations that third-party risks can be fast and furious. These disruptions, coupled with the rising sustainability standards governing the use of third parties, has increased board and investor oversight to ensure effective TPRM, pushing organizations to reevaluate their risk management efforts. Moreover, the pandemic exposed how reliant which organizations are on third parties and nth parties to ensure business continuity. In response, stakeholders are eager for increased accountability of TPRM activities and for a more coordinated and consolidated view into TPRM efforts and results.

For effective TPRM efforts, organizations should account for third party and extended enterprise partner actions to minimize disruption and promote compliance with increasing regulations. This step will demand enhanced TPRM efforts throughout due diligence and continuous monitoring to encompass ESG-related requirements for third parties and their nth parties. To create and sustain effective TPRM governance, leading organizations will increasingly designate a single primary owner of TPRM to improve the accountability of their risk management efforts. The research below explores these trends in detail.

Kind regards,

Koray Kose and Nicholas Sworek

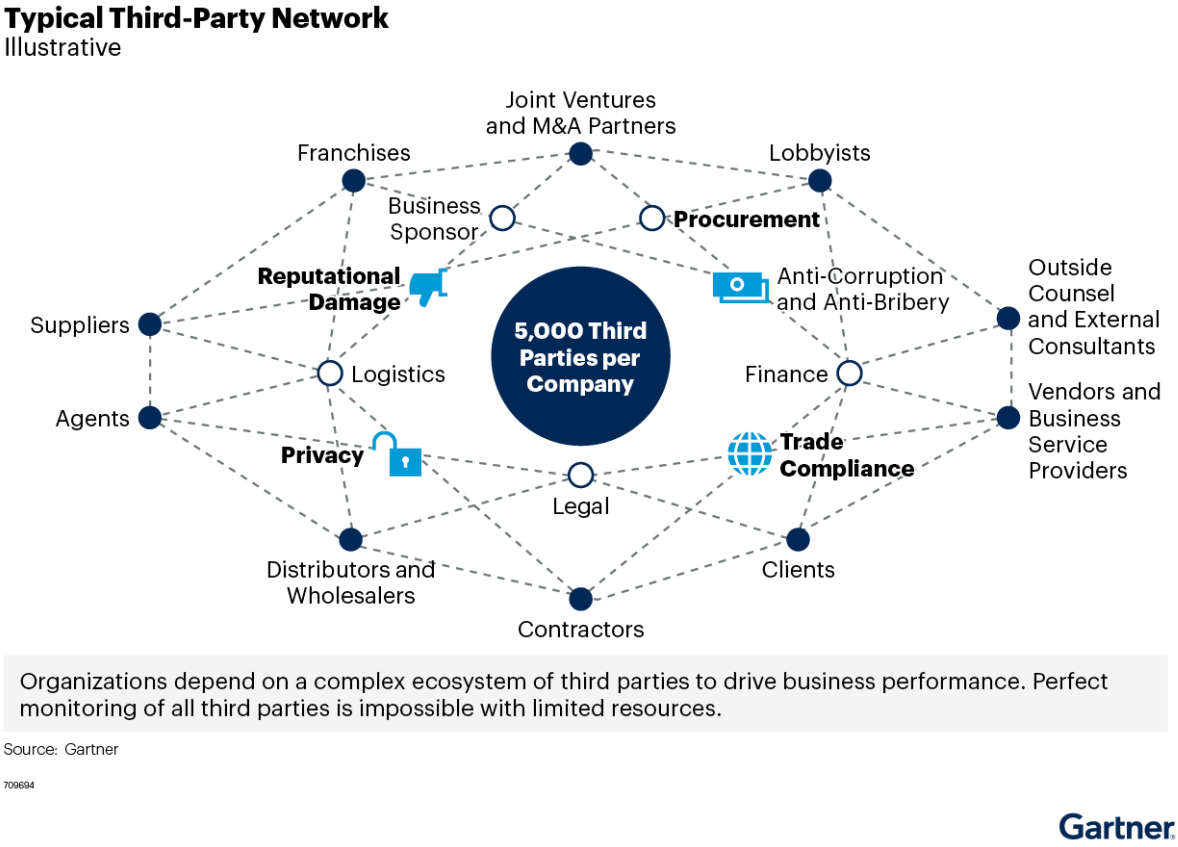
Executive Overview

Definition

This collection of research identifies the top trends in third-party risk management that will drive governance and technology investments through 2022.

One of the key magnifiers of third-party risk is an extended third-party network outside the enterprise (see Figure 1). Organizations are increasingly using third parties for business-critical purposes to improve performance and gain competitive advantage. The sheer volume of third parties makes monitoring the level of risk exposure these risks pose to the organization difficult.

Figure 1: Typical Third-Party Network

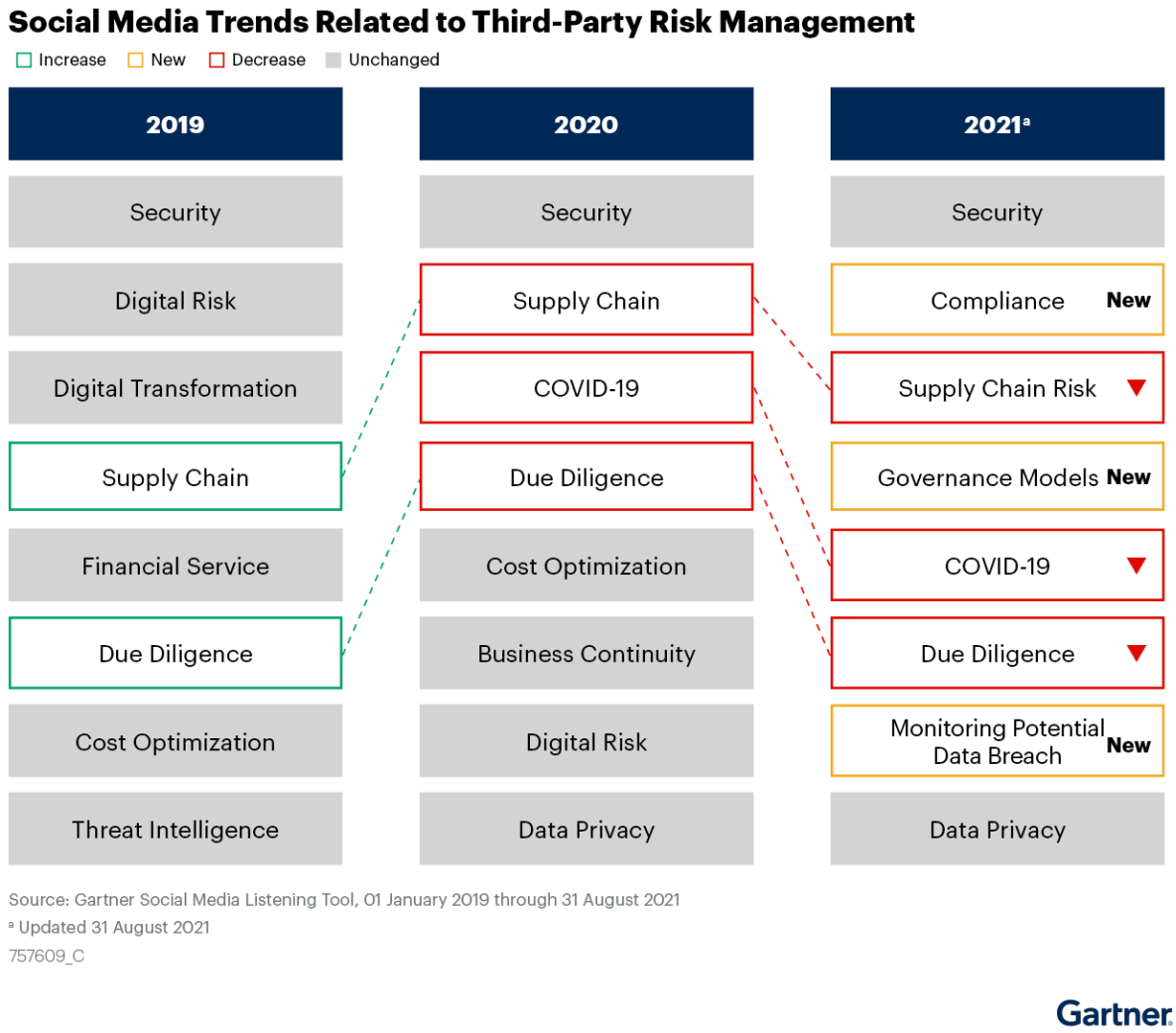


While third-party risk is one of the most pressing challenges for risk management leaders, organizations are increasingly dependent on third parties to do business, provide goods and services, and improve operational efficiency. With this growing dependency on third parties comes a heightened demand from boards and regulators for strict monitoring and rigorous controls to ensure effective risk management. However, only 28% of organizations continuously monitor third parties throughout engagement cycles; just 16% say they effectively manage third-party risks. Managing the effectiveness of compliance processes is also difficult as they vary based on the geographic and industrial regulations the organization operates in, which makes managing third-party risks harder.

Third-party risks can have severe costs and consequences for affected companies, including supply chain disruptions, vendor fraud, cyber incidents, data loss and regulatory fines that can exceed $500 million under the U.S. Foreign Corrupt Practices Act. These are just some of the risks that have resulted from increased reliance on third parties and the extended enterprise. For instance, in June 2021, the Cancer Centers of Southwest Oklahoma announced a data breach of protected health information of 8,000 patients.[1] Another such incident was noted in July 2021, when Audi and Volkswagen suffered a data breach after a vendor left unsecured data on the internet. In response to the breach, a California consumer sued the two companies for not safeguarding personal information under the Driver's Privacy Protection Act and the California Consumer Privacy Act.[2]

The drive to effectively manage third- and nth-party risks is evident through our analysis of social media trends, which suggest a focus on how organizations can increasingly ensure compliance and mitigate third-party risks throughout the relationship with more effective governance. This increased focus on compliance and governance, and a continued emphasis on security, join other trends focused on supply chain risks and monitoring potential data breaches (see Figure 2).[3]

Figure 2: Social Media Trends Related to Third-Party Risk Management



Source: Gartner Social Media Listening Tool, 01 January 2019 through 31 August 2021
[a] Updated 31 August 2021
757609_C

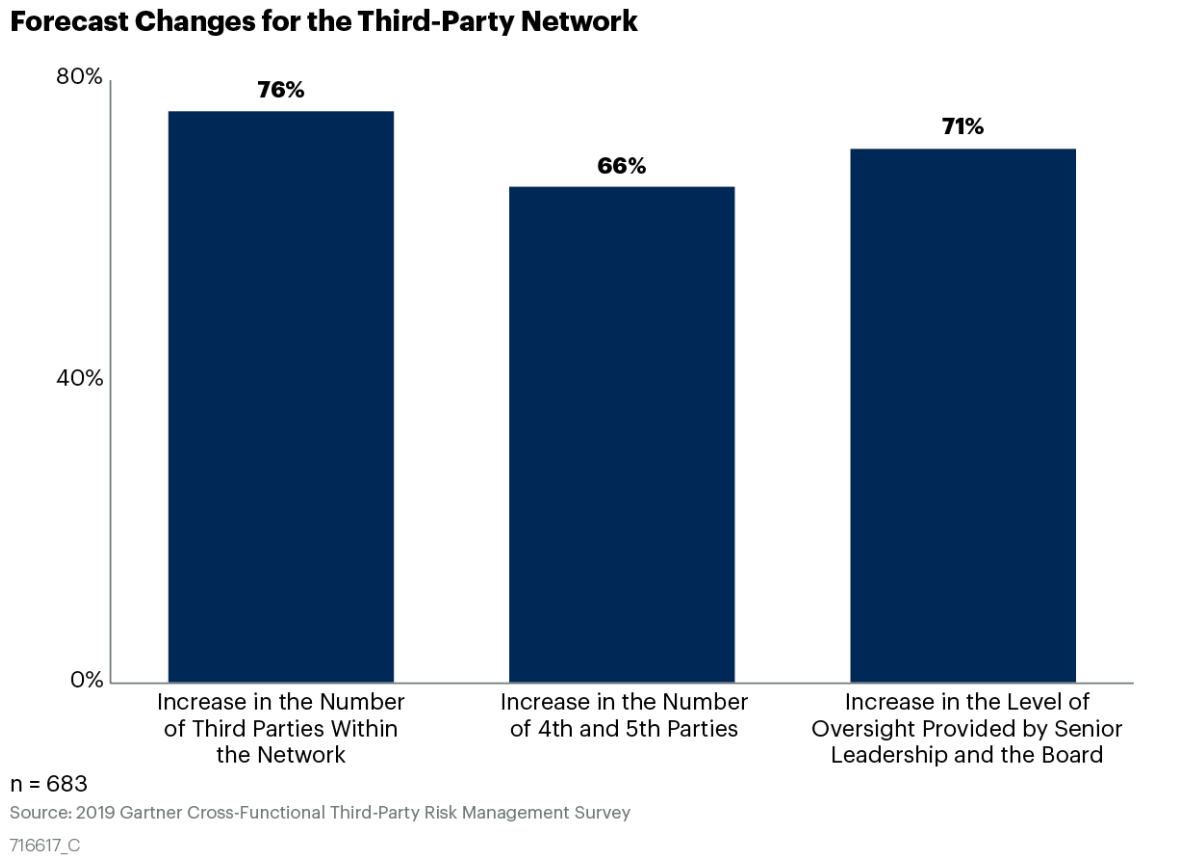
Gartner

Research Highlights

A New Wave of Legislation Focused on Fourth Parties

The third-party network continues to expand to include a number of nth parties. Seventy-six percent of organizations anticipate an increase in their third-party networks over the next three years. The increasing dependence on extended enterprise partners, coupled with growing regulatory and public oversight and macroeconomic pressures, exposes organizations to a host of new and amplified risks and compliance issues. Unsurprisingly, 71% of organizations anticipate an increase in oversight from senior leaders and boards over the next three years.

Figure 3: Forecast Changes for the Third-Party Network



In addition, organizations report having difficulty performing due diligence on third parties beyond Tier 1 (see Table 1). More than half of organizations fail to carry out sufficient due diligence on key third parties in Tier 2.

Table 1: Organizations That Seek Business Continuity Arrangements of Key Third Parties, by Tier

Tier	Yes, for Some	Yes, for All
Tier 1 suppliers	49.4%	32.5%
Tier 2 suppliers	18.5%	32.1%
Tier 3 suppliers	9%	19.2%
Tier 4 and beyond suppliers	7.6%	10.1%

Source: BCI's Supply Chain Resilience Report 2021*

Apart from increased board oversight, TPRM leaders also need to be mindful of a new wave of legislation that requires organizations to gather insights deeper in the supply chain than before. For instance, NIST has expanded the basis for fourth-party requirements and now mandates that organizations:

- Link risk management activities to the nth party's mission.
- Establish responsibility for controls throughout systems.
- Encourage use of automation to increase consistency. [4]

The U.S. Office of the Comptroller of the Currency has also proposed guidance requiring banking organizations to include information about subcontractors in their third-party monitoring efforts. [5]

To further this guidance and requirements, the EU released the Due Diligence Act, which requires due diligence of non-EU organizations in the value chain to increase their understanding of human rights and climate risks within the supply chain. Similar legislation is in the works in Germany, Switzerland, Canada and Australia.

While these regulations are not yet formulated, organizations are still required to act on them to protect themselves from unwarranted regulatory fines and penalties. This combination of potential regulations and increased board oversight is pressuring TPRM leaders. They must now rethink their due diligence requirements to perform greater scrutiny of third-party practices, particularly the level of scrutiny paid to the reputation of the third party, its nth parties and their key principles.

To manage the risks posed by their growing third-party networks, organizations must expand their technology investments and invest in smarter, more applicable solutions. In fact, our 2020 State of the Compliance Function survey indicates compliance anticipated spending 8% of its total budget on technology in 2020, compared to 4.5% in 2019. These higher spending levels occurred in response to the urgency to digitalize and manage increased workloads amid COVID-19. We've also identified this trend in supply chain counterparts that expanded their technology budgets to deal with the aftermath of COVID-19 disruptions. In our 2021 Gartner Supply Chain Risk and Resilience Survey, 58% of supply chain organizations reported an increase in their technology budgets to manage critical supply chain risks.

The requirement for contingency plans for third parties who provide critical business processes or systems has never been more evident. Security and risk management leaders must ensure actionable plans are prepared to address situations where critical third-party services are compromised.

The Impact of ESG Imperatives on TPRM

The global momentum for transparency and sustainability has created a push from boards, investors and activist employee groups for more meaningful ESG initiatives and objectives. This push has created a renewed focus on TPRM activities and application investments. The EU's Due Diligence Act has imposed new wide-ranging ESG due diligence requirements on organizations established or operating in the European Union. Further, governments are pushing organizations to improve the transparency of their climate impact reporting. For example, in May 2021, a Dutch court ruled that Shell must accelerate existing commitments in response to stakeholder dissatisfaction with Shell's rate of progress on its energy transition plans.

The U.K. has taken similar steps, requiring organizations to report on climate change by 2025. The EU has also recently rolled out regulations and reporting standards — such as the European Climate Law, Corporate Sustainability Reporting Directive and Sustainable Finance Disclosure Regulation (SFDR) — setting targets to become climate-neutral and mandating sustainability-related disclosures. As regulators move to treat climate change as a systemic financial risk, U.S.-based companies may expect mandatory disclosures as early as mid-2022. In response to these increasing regulations, nearly 25% of compliance leaders are prioritizing ESG among their top three areas to refine before 2024 to support corporate ESG initiatives and mitigate reputational and regulatory risk.

Simultaneously, over 76% of organizations are increasing the number of third parties they work with to accomplish their mission-critical priorities. [6] This increase in third parties will also pressure organizations to account for ESG-related requirements within their due diligence and continuous-monitoring processes. Fifty-two percent of organizations report compliance committees holding partial responsibility for ESG initiatives. [7] This finding implies that compliance will need to ramp up its current risk management activities to account for sustainability-related requirements.

While 45% of organizations involve compliance in performing ESG materiality assessments, and 33% of compliance functions are responsible for preparing their organizations' external ESG reporting, these figures will dramatically increase as governments continue to create ESG legislation and increase accountability. [8] As a result, CCOs will seek accurate metrics to ensure organizations are fulfilling their public commitments and publishing accurate reports and materiality assessments.

To help organizations perform these assessments, we've observed TPRM vendors providing ESG-related metrics or other related information as evident from our survey of the TPRM vendor market. In fact, over 29% of TPRM vendors are currently supporting ESG-related third-party risks, and others are looking to enhance their solutions by including support for ESG, given the rapid growth of related regulations. [9] While vendors are delivering support for ESG, CCOs should ensure the availability and quality of this data has been assessed before capturing it within their assessments.

Enhanced Focus on TPRM Governance

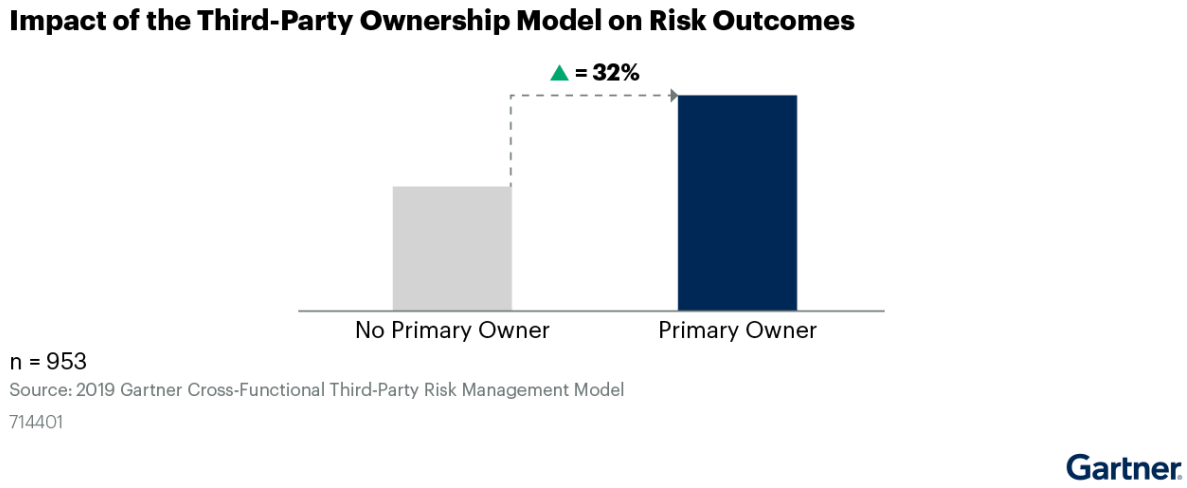
Given the heightened stakeholder oversight of TPRM initiatives, organizations are pushing for increased accountability and a coordinated, consolidated view into TPRM activities. However, organizations struggle to establish TPRM governance as risk management activities are divided within functions, with one function performing due diligence and the other conducting continuous monitoring. This separation often leads to duplicative efforts, missed opportunities for collaboration and loss of critical third-party risk information.

One method of strengthening risk management activities is to implement TPRM activity governance. These committees, or councils, bring together third-party risk owners and other subject matter experts to analyze current risks, plan for emerging ones and evaluate control effectiveness. Unsurprisingly, supply chain counterparts in over 79% of organizations have pushed to either have a risk committee or will implement one in the next two years to oversee the governance of supply chain risks. [10]

TPRM leaders should collaborate with the functions participating in TPRM oversight to establish the overarching framework and policies for TPRM governance. Having a risk committee allows organizations to effectively share critical risk management information, reduces duplicative efforts and promotes unified decision making that eventually improves risk management outcomes.

After establishing a risk committee, organizations should identify a single, primary owner responsible for TPRM. The primary owner is the function that identifies and mitigates the most critical third-party risks for the organization and requires unrestricted access to critical third-party risk information. While having several functions participate in TPRM activities improves TPRM efforts, the lack of a primary owner hinders critical information sharing, which can impact risk management outcomes. Our research shows having dedicated governance with clear ownership over TPRM not only helps reduce duplicative efforts and promotes collaboration but also improves risk management outcomes by 32% (see Figure 4).

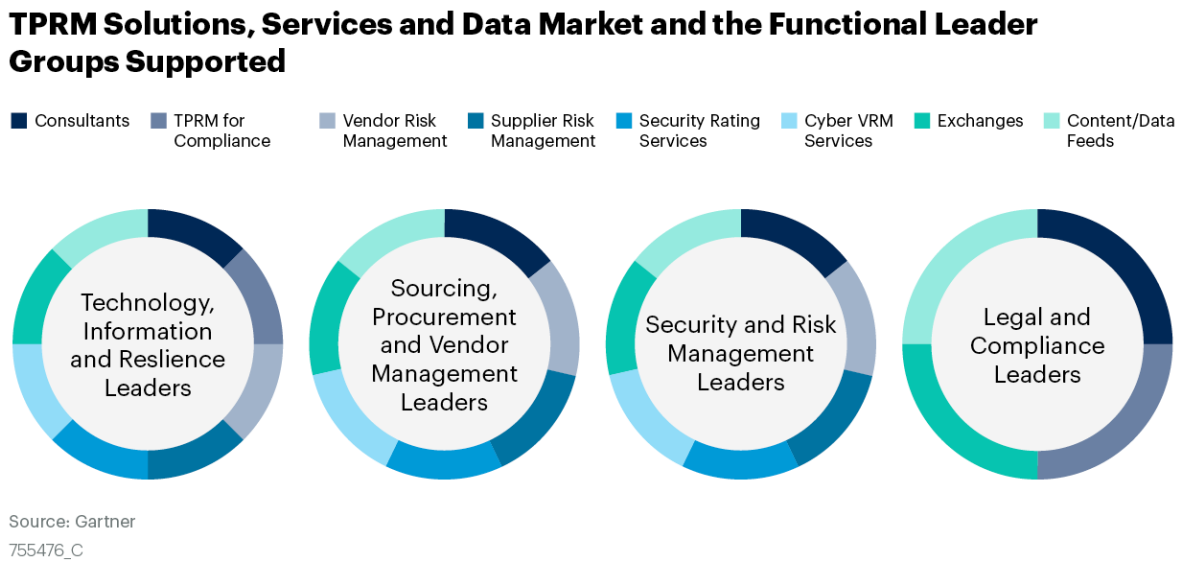
Figure 4: Impact of the Third-Party Ownership Model on Risk Outcomes



Over 60% of supply chain organizations have implemented or are implementing organizational structures with clearly defined responsibilities to manage critical supply chain risks, since the beginning of COVID-19 disruptions. [10]

Our analysis of the TPRM solutions vendor marketplace indicates TPRM solutions are marketed and primarily designed to support one or more functional leader groups (see Figure 5), perpetuating governance challenges. Many marketplace vendors provide discrete support to singular functional owners rather than support to enterprisewide primary owners of TPRM, restricting the primary owner's access to critical third-party risk information.

Figure 5: TPRM Solutions, Services and Data Market and the Functional Leader Groups Supported



Our analysis further reveals that, while vendors support some major third-party risk areas, such as information security risks, only a handful provide niche support for industry- or geography-specific risks, such as import and export practices risk. This finding implies a primary owner of TPRM will need to invest in a mix of TPRM solutions — our latest research indicates as many as nine systems — to get the support required to manage an organization's critical third-party risks. This lack of comprehensive support leads to costlier investments and investment overlaps as the primary owner requires a patchwork of systems to support TPRM efforts.

To effectively conduct TPRM activities, primary owners of TPRM require technology solutions that offer an intuitive dashboard to oversee critical third-party risks throughout the organization and an application programming interface that allows unrestricted access to risk information among functions.

Evidence

Gartner's Supply Chain Risk and Resilience, 2021: This study was conducted to understand companies' current capabilities for supply chain risk management, where improvements are most needed and where they are investing in processes, resources and technologies for the future. The research was conducted online between 19 July 2021 and 3 September 2021 among 83 respondents in Germany and six in other countries. BME partnered with Gartner to recruit the participants. The sample was augmented with recruitment efforts by social media:

- Qualifying organizations operate in the manufacturing, healthcare, natural resources, retail, transportation and logistics, utilities, and wholesale trade industries.
- Qualified participants have a role tied to a supply chain function.

The survey was developed collaboratively by a team of Gartner analysts and Gartner's Research Data, Analytics and Tools team. Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

Endnotes

[1] Oklahoma Cancer Center's EHR Server Breached by Hackers, Exposes 8,000 Patients' Data, Becker's Health IT.

[2] Audi, Volkswagen Data Breach Affects 3.3 Million Customers, Bleeping Computer.

[3] **Social Media Analytics Methodology:** Gartner conducts social listening analysis leveraging third-party data tools to complement or supplement the other fact bases presented in this document. Due to its qualitative and organic nature, the results should not be used separately from the rest of this research. No conclusions should be drawn from this data alone as it may not be entirely market representative. Social media data in reference is from 1 January 2019 through 31 August 2021, in all geographies (except China) and recognized languages. Social media sources considered for analysis include Twitter, Facebook (publicly available information only), aggregator websites, blogs, news, mainstream media, forums and videos (comments only); unless and until specified. Anindya Som Chowdhury and Fahim Talmeez from the Social Media Team contributed to this research.

[4] NIST Risk Management Framework, NIST.

[5] Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29, Office of the Comptroller of the Currency.

[6] 2019 Cross-Functional Third-Party Risk Management Survey.

[7] 2021 ESG Panel Benchmarking Survey, n = 133.

[8] 2021 ESG Panel Benchmarking Survey, n = 175.

[9] 2021 Market Guide for Third-Party Risk Management Solutions for Compliance.

[10] 2021 Gartner Supply Chain Risk and Resilience Survey.

* BCI's Supply Chain Resilience Report 2021.

Actionable, objective insight

Explore these additional complimentary resources and tools for legal, risk & compliance leaders.

eBook

Anatomy of an Effective ESG Program

Uncover the key components of a high-impact corporate environmental, social and governance (ESG) program.

Download eBook

Webinar

Aligned Assurance — The Key to Third-Party Risk Management

This virtual briefing reveals the key elements to third-party risk management (TPRM) and highlights opportunities for assurance alignment.

Watch Webinar

Case Studies

Client Success Stories

Learn how our guidance and tools have enabled legal and compliance teams to achieve stronger performance.

Learn More

How We Help

Gartner for Legal, Risk & Compliance

Discover how we can help you to achieve your mission-critical priorities.

Watch Video

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

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 Leaders
gartner.com/en/legal-compliance

Stay connected to the latest insights

Gartner®