



Third-party ecosystem: Why rethink third-party risk?

You need more information for third-party decisions and managing associated risks

The evolution of the **third-party ecosystem**

Organizations have long relied on third parties for specialty services, competitive advantage, operational efficiency, and cost-savings. But an important shift is taking place as organizations expand their third-party ecosystems to execute core activities that are critical to operations, business models, and value propositions. This in turn is intensifying risks for the extended enterprise.

As one example, the sheer number of relationships can explode as organizations rapidly adopt new operating models and outsource more core and noncore functions to third parties—cloud service providers are one prominent example. Another example is the growing demand for agility as organizations face off with new and untraditional competitors globally, including tech-savvy, digitally enabled upstarts that are disrupting entire industries. Third parties can be an important component of that agility.

And organizations are rethinking the nature of work, workforces, and workplaces as talent gaps appear and automation, analytics, and artificial intelligence (AI) increasingly augment and enhance traditionally human-performed jobs. Third parties can play a part in many of those changes.

As third-party ecosystems continue to expand exponentially, important questions are being asked by boards of directors and other stakeholders regarding the risk to the extended enterprise, including:

.....

What does our third-party population look like and where are the highest concentrations of risk?

.....

How is that risk being detected, monitored, and measured?

.....

What is being done about it?



The evolution of the **third-party ecosystem** continued

These questions might be answered by a compliance or operations leader in other areas of an organization. But when it comes to third-party relationships, no single executive or function typically has overall visibility into or responsibility for risk. For large organizations that may have tens of thousands of third-party relationships, this can create a gap in extended enterprise risk management.

The potential for, and implications of, third-party-related incidents and disruptions can be far-reaching if not properly assessed, monitored, and managed. And, unless organizations change the way they govern third-party risk across their interconnected ecosystems, their business will likely continue to be disrupted. A recent survey of more than a thousand executives at organizations around the world revealed that:

87%

faced a disruptive incident with third parties in the preceding three years

28%

faced a major disruption to all business functions because of a third-party incident

26.2%

suffered reputational damage as a result of third-party actions

23%

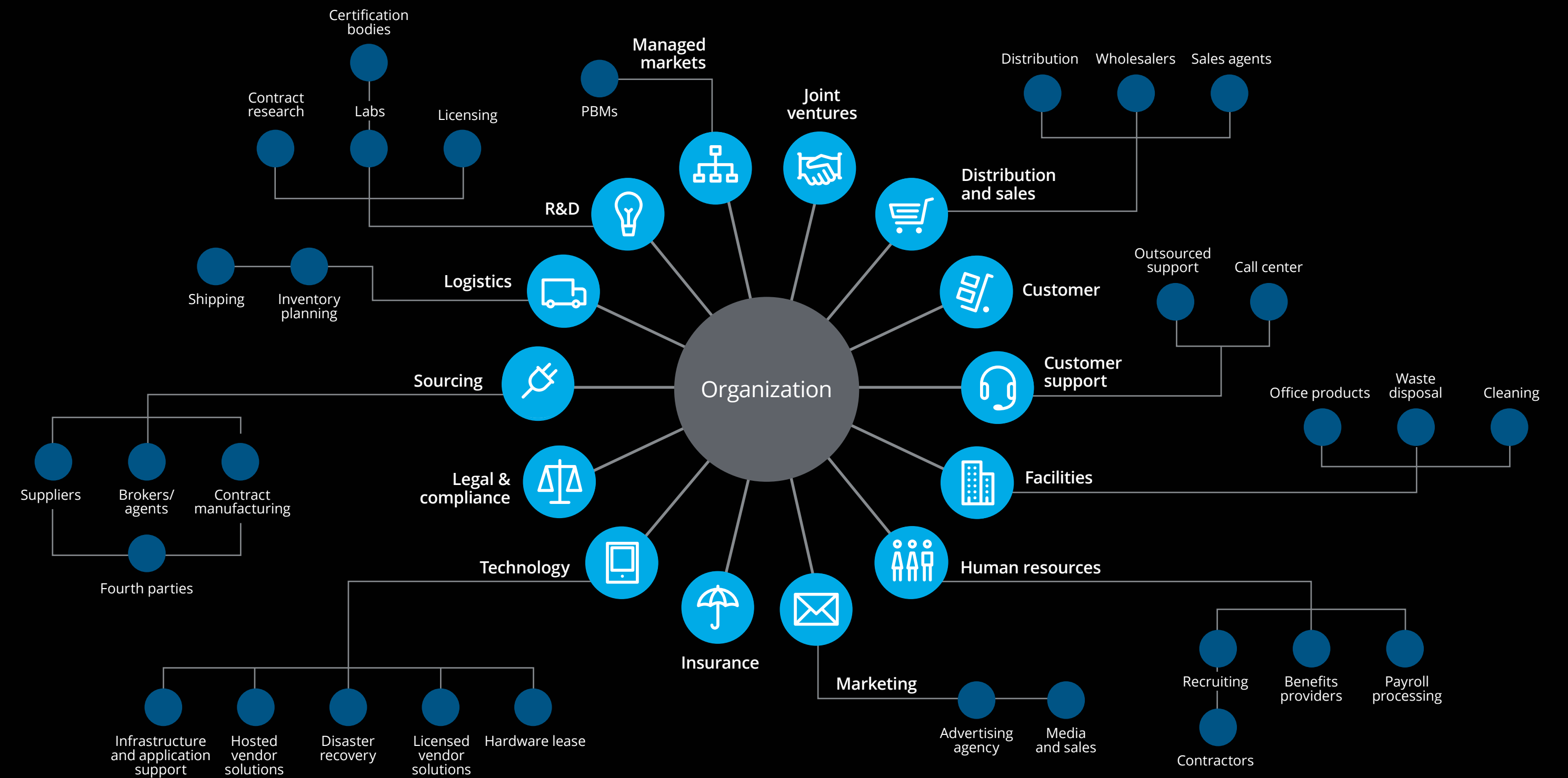
have been **non-compliant with regulatory requirements**

21%

experienced **breaches of sensitive customer data** due to third-party actions

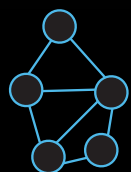
According to the survey, in some industries, companies have faced fines and restitution nearing \$1 billion for incidents related to third parties.

Third-party ecosystem



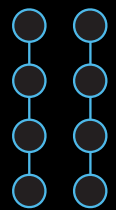
Third-party risk management is not one-size-fits-all

Some organizations have set up third-party risk management (TPRM) programs to help increase their visibility into third-party relationships and activities. Such internal TPRM programs generally follow one of three operating models:



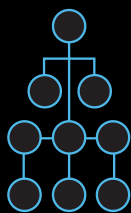
Distributed

Each business or geographic unit manages TPRM separately



Siloed

TPRM activities may span the organization, but different teams manage them based on types of risk



Federated

TPRM activities remain divided among different teams or units but are subject to planning and oversight from a single group

Each model has its limitations. For example, bound by resources at the business-unit level, the **distributed** model may be subject to staffing, technology, scalability, and other constraints. It can also be inefficient, requiring each business unit to ramp up a TPRM program and train people to run it. Processes, governance, and controls for each type of risk can vary from one program to another, making them hard to compare. Finally, because they reside farther down in the organization, distributed TPRM programs can struggle to gain executive and board-level support.

Meanwhile, with **siloed** and **federated** models, vendor onboarding can take up more and more time as third-party relationships proliferate. Risk reporting, metrics, and data can be incomplete, inconsistent, and unreliable, and may lack quality. Duplication of effort can still be an issue, as well.

How a managed services model can help **drive clarity and accelerated outcomes**

In light of the challenges of developing and maintaining internal third-party risk management programs, more organizations are turning to a managed services model. This model can help improve the management of extended enterprise risk by centralizing TPRM planning, oversight, and execution into a single group.

This approach can:

- provide stakeholders with a single point of transparency and visibility into third-party risk so they can effectively manage risk profiles across the enterprise
- facilitate accelerated outcomes with access to true risk domain knowledge, technology, and appropriate talent
- roll up risk data into a single report to quantify where the highest risks are, what is the nature of the risks, and what is being done to address it




How a managed services model can help drive clarity and accelerated outcomes continued


Additionally, a managed services model can:

- Create greater consistency in third-party risk management (TPRM) processes across business units
- Help establish a framework and be readily scaled to onboard more third parties to the organization’s portfolio
- Provide relevant insights that help the organization create economies of scale by having more visibility into third-party performance
- Bolster extended enterprise risk management capabilities with much needed skills, tools, techniques, and processes to take on the toughest part of TPRM—reducing operational, regulatory, reputational, strategic, and technological risks
- Optimize staffing so that internal teams can focus on other mission-critical initiatives


As a result, organizations can expect:



The ability to quantify and reduce risk exposure through improved risk mitigation strategies, TPRM effectiveness, and consistency



Improved visibility into the portfolio of third-party relationships for informed decision making



Productivity gains through more coordinated TPRM activities while improving risk posture through analytics and benchmarking against industry standards

A managed services model can yield benefits that resonate with senior leadership and the board while reducing risks across the various domains affecting your organization.

Let's talk

Kristian Park
EMEA leader | Extended
Enterprise Risk Management
Global Risk Advisory
Deloitte UK
+44 20 7303 4110
krapark@deloitte.co.uk

Dan Kinsella
Americas leader | Extended
Enterprise Risk Management
Partner | Risk & Financial
Advisory
Deloitte & Touche LLP
+1 402 997 7851
dkinsella@deloitte.com

Suzanne Denton
Managing director |
Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 436 7601
sudenton@deloitte.com

Kevin Gallagher
Managing director |
Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 436 6072
kevgallagher@deloitte.com

Theresa McCluskey
Solution specialist
Risk & Financial Advisory
+1 980 312 3764
tmcccluskey@deloitte.com



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.