Deloitte.

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**

Organisations have long relied on third parties for specialty services, competitive advantage, operational efficiency, and cost-savings. But an important shift is taking place as organisations 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 organisations rapidly adopt new operating models and outsource more core and non-core functions to third parties (and fourth parties)—cloud service providers are one prominent example. Another example is the growing demand for agility as organisations face off with new and untraditional competitors globally, including tech-savvy, digitally enabled start ups that are disrupting entire industries. Third parties can be an important component of that agility.

Organisations 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 organisation. But when it comes to third party relationships, no single executive or function typically has overall visibility into or responsibility for risk. For large organisations 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 organisations 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 organisations 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

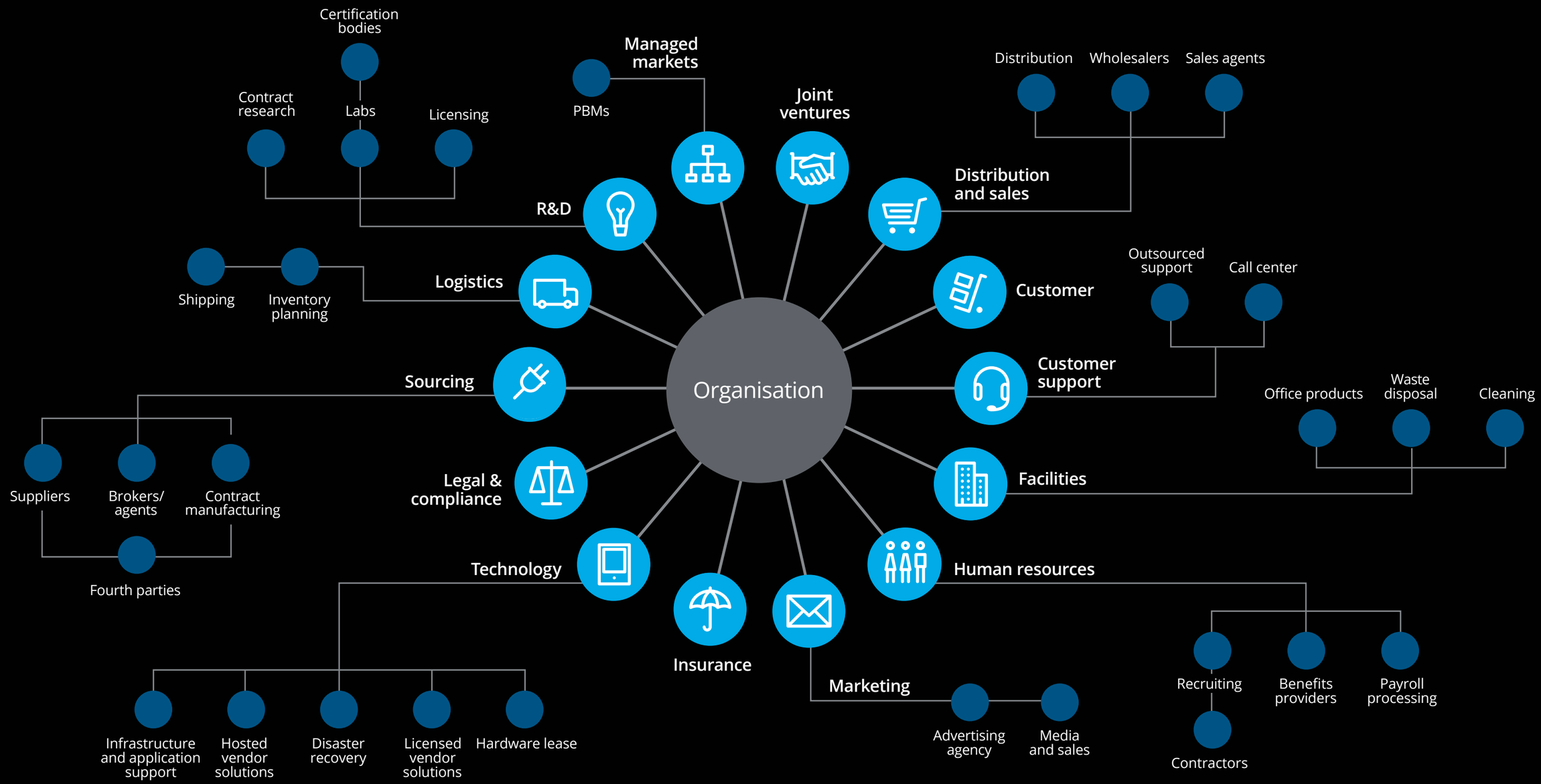
23%
have been **non-compliant with regulatory requirements**

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 US$1 billion for incidents related to third parties.

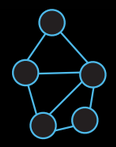
[1] Adapted from "Deloitte Touche Tohmatsu Limited's 2018 EERM Survey," https://www2.deloitte.com/global/en/pages/risk/articles/third-party-risk.html

Third party **ecosystem**



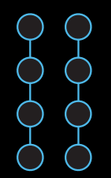
Third party risk management **is not one-size-fits-all**

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



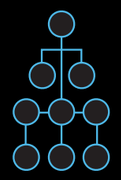
Distributed

Each business or geographic unit manages TPRM separately



Siloed

TPRM activities may span the organisation, 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 programme and train people to run it. Processes, governance, and controls for each type of risk can vary from one programme to another, making them hard to compare. Finally, because they reside further down in the organisation, distributed TPRM programmes 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 programmes, more organisations are turning to a managed services model. This model can help improve the management of extended enterprise risk by centralising 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
- roll up risk data into a single report to quantify where the highest risks are, what the nature of that risk is, and what is being done to address it
- facilitate accelerated outcomes with access to true risk domain knowledge, technology, and appropriate talent

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 organisation's portfolio
- Provide relevant insights that help the organisation 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
- Optimise staffing so that internal teams can focus on other mission-critical initiatives

As a result, organisations 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 impacting your organisation.

Why Deloitte's Third Party Management solution?

Whether your organisation has a large, well-established third party ecosystem or is in the early stages of developing third party relationships—or anywhere in between—Deloitte's Third Party Risk Management solution is designed to help you improve the health of your programme, including risk profile and compliance.

Our consistent, efficient, and reliable solution is built around industry-leading practices and processes, along with sophisticated use of both proprietary and widely available technologies. We deliver these capabilities to you through intuitive, user-friendly analytics dashboards that help you sense, assess, analyse, and monitor third party risks and offer important insights for risk-assessed decision making. Our technology platform also provides corporate and unit-level third party risk performance improvement tools and extensive reporting capabilities.

Deloitte's Third Party Risk Management solution can provide risk assessment results and other relevant insights to help you make more informed decisions about contracting with third parties and help arm you with strategies for managing and mitigating potential risk.

How it **works**

Deloitte's Third Party Risk Management solution is designed to streamline the TPRM process, from third party engagement, risk assessment, selection, and input through contract development and ongoing monitoring. Our solution includes:

Third party screening

Identifying third party risks using advanced analytics and AI on data harvested from the internet and proprietary databases

Background checks

Uncovering risk indicators within public and private databases through broad-based checks, including detailed research into suppliers, key individuals, and ultimate beneficial owners, conducted by experienced investigators

Third party questionnaires

Analysing third party policies and procedures through data collected directly from third parties regarding their control environment, such as policy, process, and capability; the questionnaire scope is aligned with regulatory and stakeholder expectations

On-site inspections

Conducting onsite inspections of the third party's risk control environment and detailed risk assessments, which are conducted by Deloitte professionals with deep domain and industry knowledge

Monitoring

Reporting and helping to mitigate risks to your extended enterprise through ongoing analysis and dashboard visualisation of various internal and external data sources to identify new and emerging issues in the third party portfolio

How it **works** continued

From cyber security to anti-bribery, our solution is flexible and responsive to the various risk domains that are most important to your organisation. We offer:

A broad-based view of risks and third parties through a central global repository with an executive dashboard and benchmarks against industry standards

Standardised processes, applied consistently across all markets and organisations, for third party risk sensing, scoring, and monitoring

Extensive and reliable insights for risk-assessed decision-making supported by real-time data for integration with functions such as procurement, risk, compliance, IT, and others

An intelligent technology platform that automates processes and aggregates risk data about your third parties to provide risk intelligence

Access to subject-matter knowledge from Deloitte professionals with deep cyber and third party risk domain experience

Why Deloitte?

We have created an integrated, end-to-end TPRM programme that can be applied across your various third party entities and risk domains with access to:

75 dedicated **delivery centers**

17,000+ **risk practitioners** around the world

Predefined processes for planning, scheduling and execution, reporting, and quality management

A technology architecture designed to be **robust, scalable, and secure**

Improve control over your organisation's third party risks and performance

As the pressure to innovate rises and enterprise networks continue to expand, third parties will move ever closer to mission-critical operations. Now is the time to turn ad-hoc enterprise risk management into a streamlined process for making more effective decisions about the third parties you work with—not only because of what they can do, but also because of who they are and the risks they may bring to your relationship.

Does your organisation:

- Lack visibility into and understanding of risks potentially posed by your relationships with many types of third parties?
- Want greater visibility with regard to third party performance and risks?
- Need to improve operational costs, process efficiencies, and organisational agility associated with your third party relationships—all while gaining greater control over related risks?
- Want to be confident that third parties are compliant with your organisations' policies—and their own—based on government regulations and industry requirements?

Look at risk domains **through a third party lens**

Executives, boards, and other stakeholders are usually well-aware of the risk domains their organisations face. But those domains take on a different complexion—and must be considered differently—when it comes to third party relationships.

Deloitte addresses a broad range of **20+ risk domains**. Below are illustrative examples.

Information and cyber security

Is your organisation's data adequately protected from accidental or malicious alteration or destruction and unauthorised access or disclosure when it's used or stored by a third party?

Fraud and corruption

How could a third party's engagement in unlawful business practices or criminal behaviour such as money laundering, bribery, or fraud adversely impact your organisation?

Financial health

If a third party suffers financially and cannot deliver a stable service or product, what operational implications could there be for your organisation?

Data privacy

Are you confident that third parties are complying with your organisation's own standards and legal and regulatory standards for the handling and protection of personal and sensitive data?

Africa Contacts

For more information, please contact

Southern Africa

Navin Sing
Managing Director:
Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Sisa Ntlango
Risk Advisory Africa Leader:
Internal Controls & Assurance
Mobile: +27 82 920 3677
Email: sntlango@deloitte.co.za

Nombulelo Kambule
Associate Director:
Risk Advisory Southern Africa
Mobile: +27 82 549 8603
Email: nkambule@deloitte.co.za

Nkateko Mabaso
Senior Manager:
Risk Advisory Southern Africa
Mobile: +27 72 288 3990
Email: nkmabaso@deloitte.co.za

Central Africa

Tricha Simon
Risk Advisory Regional Leader:
Central Africa
Mobile: +263 772 234 932
Email: tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory
Central Africa
Mobile: +263 772 263 016
Email: rdean@deloitte.co.zm

East Africa

Julie Akinyi Nyangaya
Risk Advisory Regional Leader:
East Africa
Mobile: +254 72 011 1888
Email: jnyangaya@deloitte.co.ke

Urvi Patel
Director: Risk Advisory East Africa
Mobile: +254 71 158 4007
Email: ubpatel@deloitte.co.ke

West Africa

Anthony Olukoju
Risk Advisory Regional Leader:
West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory
West Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Authors

Kristian Park
EMEA Leader | Extended Enterprise Risk Management
Global Risk Advisory
Deloitte UK
+44 20 7303 4110
krpark@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
tmccluskey@deloitte.com

Deloitte.