servicenow. | EY
Building a better
working world

Managing risk in the extended enterprise

Trends and challenges in third-party risk management

Table of contents

Executive summary

Today's pace of life demands instant transactions, frictionless access to information, and seamless user experiences. Our lives and work are becoming more entwined with technology—and as a result, enterprises are operating in an increasingly interconnected environment.

As these organisations embrace digital transformation and new ways of working, they are relying on third-party vendors to enable their growth. These partnerships can play a crucial role in helping businesses to stay agile and competitive—but they also have the potential to expose the enterprise to new risks.

At the same time, regulations and standards concerning third-party relationships are also evolving. Due to increasing globalisation and outsourcing complexity, many organisations are struggling to stay up to date with changing regulations and guidelines.

When they look at third-party risk management (TPRM), they tend to focus on cybersecurity. But that's only one piece of the larger picture. Through their work, third parties often become familiar with confidential business information, or they may gain physical access to company facilities.

Despite these emerging challenges, many companies have stabilised or reduced their TPRM programme spending, causing many to challenge their operating models and overall programme scope. Still, executives, boards, and regulators are asking for more detailed reporting and insights on third-party risk.

In this complex landscape, it's more important than ever for risk leaders to recognise that, while the organisation can outsource business processes, it can't outsource all liability. No enterprise exists in isolation—and as third-party relationships increase, anything that impacts them can impact you.

Types of third-party risk:

Cyber: Risk to your organisation's security due to deficient third-party cybersecurity controls

Reputational: Impact to your brand and reputation due to an event at a third party

ESG: Third-party risks related to the environment, socio-economic factors, corporate responsibility, diversity and inclusion, and community investment

Financial: Risk that the third party cannot continue to operate as a viable entity

Geopolitical: Legal, regulatory, socio-economic, and political considerations related to doing business in a specific country

Privacy: Data loss or compromise due to deficiencies in the third party's privacy controls

Operational: Risk that a third party fails to meet the organisation's service or product delivery needs

Fourth party: Risk to the organisation by parties engaged by your third parties, including on your behalf

Regulatory and compliance: Risk that a third-party fails to comply with a required law or regulation

Business continuity and resiliency: Risk of third-party failure that prevents the continuation of business as usual

Key trends in third-party risk management

In its 2022 *Global Risk TPRM Survey*, EY and Oxford Economics surveyed 500 institutions with a TPRM function in various sectors, including:

- Banking
- Insurance
- Health science and wellness
- Technology
- Media and entertainment
- Consumer products
- Retail

The survey found that today's organisations are working to do more with less, even as they grapple with a continuously expanding risk universe. And to do this, they're reimaging their approaches to TPRM.

The survey uncovered trends that fell under four broader themes:

New approaches

Organisations are seeking more effective governance, programme coverage, operating models.

Ecosystem expansion

The challenges of managing growing third-party networks can result in visibility gaps or assessment fatigue.
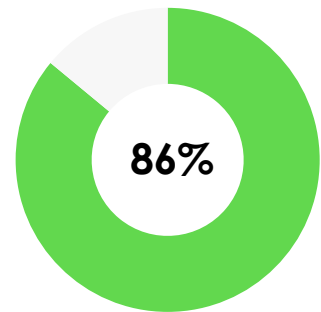
Resource prioritisation

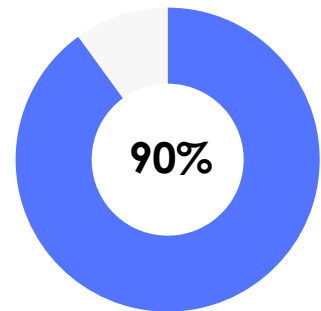Businesses are asking how they can best deploy resources to manage risk.
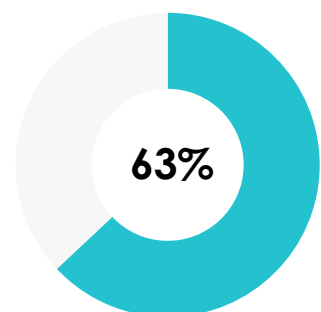
Transformative technology

Companies are working to realise the value of new technology for TPRM.

86%

of organisations report that delays and lack of coordination between internal stakeholders and TPRM are their top pain points

90%

of organisations have directly invested in their TPRM programmes, improving reporting, deepening their understanding of risk ,and aligning skillsets

63%

of organisations plan to integrate external data providers and automation to better manage inherent risk assessments in the next 2-3 years

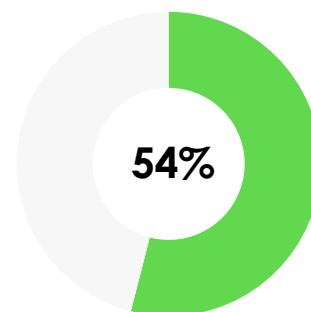**Source:** EY, *Global Risk TPRM Survey*, 2022 Highlights

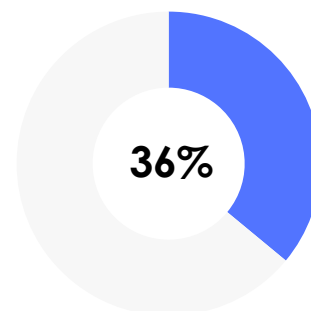# Evolving governance, programme coverage, and operating models

With the integration of managed services, market utilities, and consortiums into risk management, strong governance and programme execution are essential. But efforts to strengthen risk activities are often complicated by the fact that, in many organisations, there is a lack of clarity around who "owns" TRPM activities.

Under these conditions, it can be difficult to engage internal stakeholders and educate them on their roles and responsibilities regarding TPRM. To address the confusion, enterprises are increasingly moving to integrate their TPRM programmes into a single platform through which standards are set and maintained—typically within procurement or operational risk. This model creates clear responsibilities and accountability while streamlining the more consistent application of policies and standards.
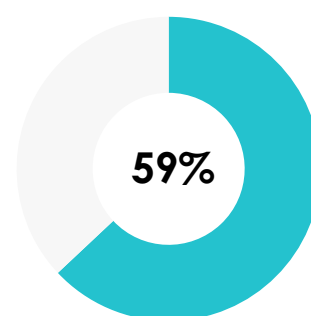
A centralised governance approach enables the management and proper oversight of an expanded third-party ecosystem, including non-traditional third parties that often do not have sufficient coverage under traditional risk management approaches.

54%

of organisations report having a centralised structure

36%

of organisations report having a hybrid structure

59%

of organisations plan to adopt a more co-sourced arrangement within the next 2 – 3 years

Source: EY, *Global Risk TPRM Survey*, 2022 Highlights

Third-party ecosystems continue to grow, creating more uncertainty and less control.

Distributors
Outsourcers
Resellers
Consultants
Suppliers
Affiliates
IT software vendors
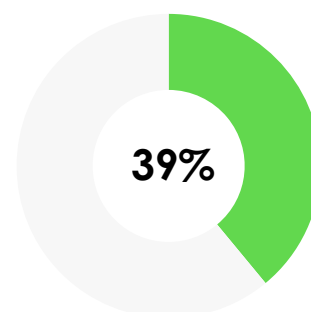
The growing third-party risk ecosystem

Enterprises across various industries (including banking, insurance, health science and wellness, technology, media and entertainment, and consumer products and retail) are working with a wider and deeper network of third parties than ever before—and the risk universe will only continue to expand in the coming years.

The complexity of managing risk for these growing third-party networks can lead to visibility gaps or assessment fatigue—especially in organisations that are still using siloed, manual TPRM tools and processes.

In the face of the daunting task of managing these risks, organisations find that they must prioritise which third parties are most critical—and they're asking how best to prioritise assessments of partners that provide critical services or handle sensitive data.

Implementing a risk-based approach for assessing third parties can allow businesses to decrease the number of control assessments they must perform. EY's survey found that, for most respondents, their three most important criteria in defining critical third parties were:

- Financial impact
- Criticality of the business process supported by the third party
- Sensitivity of the data involved

39%

of organisations assess all third-party entities within a single TPRM programme

Source: EY, *Global Risk TPRM Survey*, 2022 Highlights
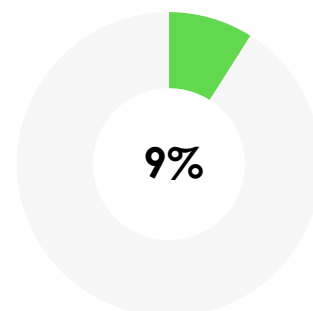
Rethinking assessments and resource deployment

In the aftermath of the COVID-19 pandemic, and with the prospect of a global financial downturn looming in the future, organisations are feeling the pressure to deliver greater value without increasing their spend on TPRM efforts.

To do this, they are increasingly implementing cross-functional integration of their cyber, procurement and operational risk programmes supported by a single technology enabler to improve visibility and process optimisation. While most established TPRM programmes align with these internal functions, many still operate in silos, degrading the value of TPRM and increasing the total cost to execute efficient TPRM. And a lack of communication between functions can leave the organisation without an accurate end-to-end view of the third-party risk environment.
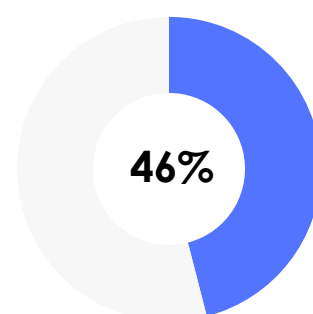
Organisations that successfully implement an integrated risk management approach will be more resilient and better prepared for uncertainty. With a collective view of risk, they can more effectively prioritise assessments and ensure that their activities align with the compliance, legal and technology functions within the enterprise.

Additionally, this approach empowers organisations to link their internal controls to third-party impact, improving overall quality and enterprise risk management.

As a result, third-party populations can be more effectively tiered for risk, and organisations can be more selective in determining the scope and frequency of their assessments and continuous monitoring. They can set higher standards for critical providers—and be more targeted and thoughtful with the "critical" designation.

9%

of in-scope third parties, on average, had a control assessment performed in the last year

46%

of organisations have terminated a third party due to findings or issues identified during assessment

Source: EY, *Global Risk TPRM Survey*, 2021

Transformative technology and automation

In this rapidly changing risk environment, it can be difficult to keep pace with the rate of change. Businesses often struggle to integrate their external data providers, and the complexity of TPRM processes can lead to assessment fatigue.

Meanwhile, the use of risk and threat intelligence tools is becoming increasingly common—but organisations have yet to unlock the full value of advanced analytics, artificial intelligence, robotics process automation, and blockchain.

This is, in part, because many organisations are still using outdated tools like spreadsheets and email to manage third-party risk. The reliance on legacy methods impedes visibility, scale, and efficiency for businesses and suppliers.
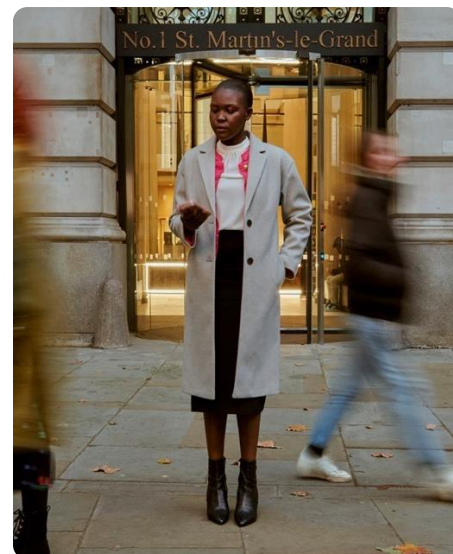
As a result, businesses are increasingly discovering that the challenges of transforming their TPRM model into centralised model are vastly outweighed by the benefits. To gain more efficient data and processes, organisations are increasingly shifting to this more unified approach.

Today's enterprises must reimagine their methodologies, maturing their TPRM programmes to gain efficiencies and real-time oversight. By automating routine processes, they can:

- Improve risk monitoring activities.
- Create more transparent workflows.
- Drive more efficient TPRM programmes.
- Expedite business outcomes.
- Reduce assessment fatigue.

Together, ServiceNow and EY streamline the flow of information, remove friction and deliver richer human experiences.

Our approach to workflow automation unlocks the potential for organisations to become more dynamic and innovative to drive business performance and growth.

Outcomes

With the versatility of ServiceNow and EY's business acumen, we help you manage risk more effectively.

Managed risk taking—so you can make informed decisions about which risks are acceptable

Increased buying power from incorporating a view of risks in negotiating and managing relationships

Increased business agility with vendor risk embedded into business workflows and capabilities that allow you to collaborate with vendors directly

Improved resiliency posture through continuous monitoring and enhanced risk mitigation through advanced technology

Managing third-party risk proactively with ServiceNow and EY

ServiceNow and EY combine ingenuity with a leading digital workflow platform, innovating together to deliver workflow automation and integrate your TPRM processes. As a result, you can get better connectivity across systems, greater resource efficiency, and seamless, human-centric processes.

Supported by ServiceNow's Vendor Risk Management (VRM) application, our approach can help your organisation:

Gain a complete view of your third-party vendors, including the parent-child relationships of the global organisations that support your operations or supply chain.

Apply a risk-based approach by assessing the specific services or products provided by third parties at the engagement level or the vendor level.

Profile third parties across multiple risk areas and trigger due diligence automatically, including scoping control-based questionnaires.

Maintain a complete log of interactions with third parties, including communications and supporting documentation.

Integrate your data to provide a complete profile of third parties, leveraging threat intelligence as well as internal and external data sources.

Provide a streamlined workflow to accept risk or remediate risk in collaboration with third parties

Integrate third-party risk processes into upstream and downstream activities for a seamless user experience

Improve supply chain resilience and sustainability supported by ServiceNow ESG and ServiceNow Operational Resilience

Key outcomes

With the versatility of ServiceNow and EY's business acumen, we help you manage risk more effectively and realise a range of benefits including:

Managed risk taking

Make informed decisions about which risks are acceptable.

Increased buying power

Incorporate a view of risks in negotiating and managing relationships.

Increase business agility

Embed vendor risk into business workflows and capabilities that allow you to collaborate with vendors directly.

Improved resiliency posture

Implement continuous monitoring and enhanced risk mitigation through advanced technology.

How will you erase the bureaucracy and invigorate your business?

To adapt to the continuously expanding universe of risk, enterprises need to re-assess and adopt an approach to TPRM that proactively identifies risk, rather than reacting to adverse events after they happen.

ServiceNow provides a global, scalable, and trusted platform that drives better transparency and monitoring of third-party risk—simplifying data sharing and reporting while providing rapid time to value.

By adopting a single platform, organisations can seamlessly embed TPRM and compliance into workflows to integrate and automate risk management activities across the enterprise.

EY teams help businesses make better-informed decisions faster about third parties by examining risk from every angle—providing the insights organisations need to identify the partners that will create better long-term value for the business.

Together, ServiceNow and EY help businesses to manage third-party risk more intelligently and efficiently—so business works smoother, employees work smarter, and customers don't have to work at all.
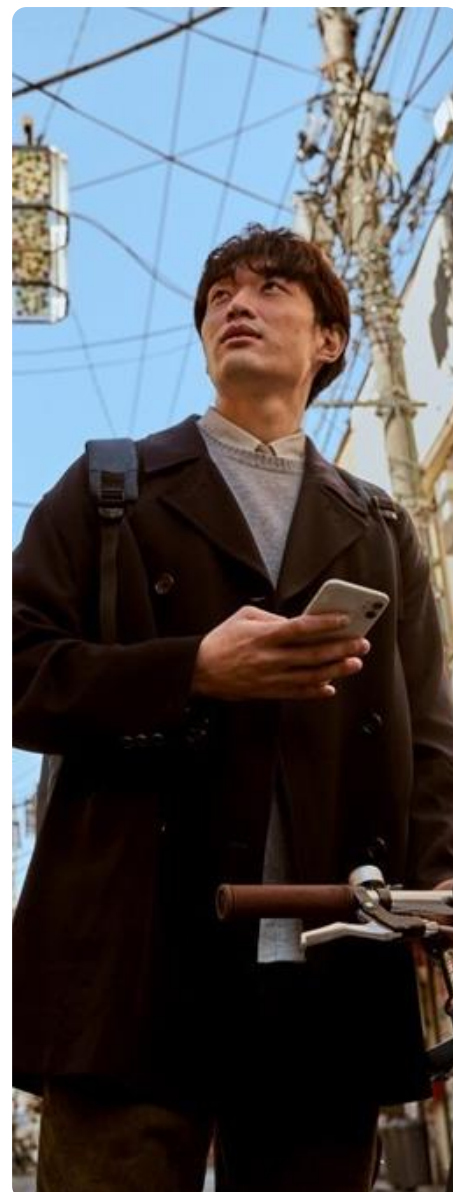
Contacts

Gaurav Mahendru

ServiceNow Senior Manager,
Solutions Consulting – Technology Workflows
gauravkumar.mahendru@servicenow.com

Chee Kong Wong

EY Asia-Pacific Risk
Consulting Leader
chee.kong.wong@au.ey.com

Learn More

servicenow. | EY
Building a better working world

servicenow.com