In an uncertain world, how do you see every angle?

2023 EY Global Third-Party Risk Management Survey

The better the question.
The better the answer.
The better the world works.

EY
Building a better working world

OXFORD ECONOMICS

Contents

Executive summary

The value of third-party risk management (TPRM) is underscored by the results of the EY 2023 Global Third Party Risk Management Survey. Nine in 10 respondents say their organization has directly invested in their TPRM program. Those that have report a better understanding of risk and optimized capabilities and effectiveness.

Companies recognize that each third-party relationship brings potential risk, said Joseph Kelly, EY Oceania Third Party Risk Leader. "The only way to completely zero out your third-party risk is to not work with third parties, but that's not going to happen. So it's more about, 'How do you identify, manage and mitigate?' We're moving from the era of just identification into management and mitigation."

While some organizations rely on email questionnaires, manually updated spreadsheets and sample data to track third parties, many organizations are turning toward a centralized and data-driven approach to support strategic risk management decisions. They want to capture a sophisticated picture of overall risk, and they're using additional capabilities, such as automation and external reports that deliver real-time information.

Using this approach, leading organizations are now able to test thousands of third parties, rank them across risk domains for criticality, and then develop a focused response, said Scott McCowan, EY Americas Risk Management Leader. "As companies continue to lean into their third-party network, a data-driven approach to screening allows for better coverage, real-time data, continuous monitoring and targeted assessment activities."

90%

of respondents are investing to improve their TPRM program's effectiveness

While TPRM programs have traditionally been driven by regulatory pressures, other forces — such as data breaches, supply chain disruptions and board pressures — have emerged as additional drivers for TPRM program investment in recent years, said Kanika Seth, EY Global Financial Services Third Party Risk Leader. Survey respondents ranked cybersecurity and digital risk as the top risk domains included in their risk inventory reporting, followed by strategic risk, financial viability risk and environmental, social and governance (ESG) and sustainability risk. Organizations are also reexamining risk governance and integrating ESG commitments into third-party risk assessments.

The next opportunity is to turn TPRM into a strategic enabler, Kelly added. "Organizations have been sitting on a rich bed of data."

About the survey

The 2023 EY Global Third-Party Risk Management Survey

In collaboration with Oxford Economics, we surveyed more than 500 institutions to understand how organizations manage third-party risks embedded in their network of suppliers, external business relationships and other types of third-party interactions.

The survey covers a range of topics, including organization, governance and oversight, nontraditional third parties and subcontractors, due diligence and ongoing monitoring, data and technology, costs and investments, third-party population and risk tiering, environmental, social and governance (ESG), TPRM maturity, customer response and resiliency.

The 50-question survey was answered anonymously, and the EY organization was not identified as the sponsor.

Participants were split representatively across various sectors, including banking and capital markets, consumer products and retail, financial services, government and public healthcare, insurance, power and utilities, professional services, technology, wealth and asset management.

The organizations have more than US$250 million in revenue.

- Seventeen percent of organizations are listed in the Fortune 500.
- Companies are headquartered in Australia, Canada, China, France, Germany, India, Italy, Japan, the Nordics, Singapore, Spain, the UK and the US.
- Less than one-third of participants have run a TPRM program longer than five years.

Q **Which risk domains are included in your risk inventory reporting?**

Select all that apply.

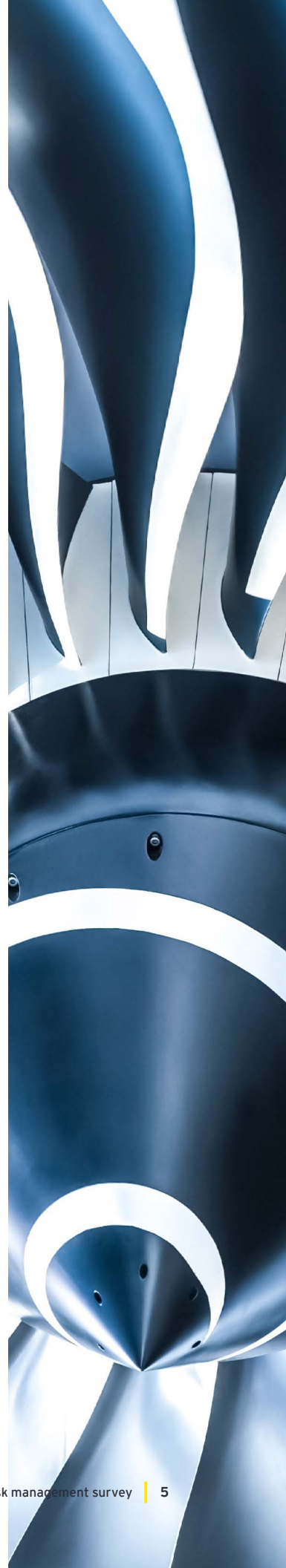
61%	Cybersecurity and digital risk
43%	Strategic risk
43%	Financial viability risk
42%	ESG and sustainability risk
39%	Privacy risk
39%	Regulatory and compliance
38%	Operational risk
37%	Business and technical continuity and resiliency
32%	Fraud
31%	Brand and reputational risk
15%	Geopolitical risk
14%	External events e.g., pandemic, war, Log4j
10%	Subcontractors
9%	Concentration risk

“

The only constant today is change and disruption. As companies try to do more with less, key operational, financial and compliance-related functions are increasingly placed in the hands of third parties.

As companies continue to lean into their third-party network, a data-driven approach to screening allows for better coverage, real-time data, continuous monitoring and targeted assessment activities.

Scott McCowan
EY Americas Risk Management Leader



1 Financial services area step ahead

Financial services industries tend to have more mature third-party risk management programs than other industries. This is because financial services organizations — including banking and capital markets, insurance, and wealth and asset management — are much more regulated across the globe.

Financial services organizations are also more likely to use a centralized TPRM program structure (62% compared with 46% of nonfinancial services and 54% of respondents overall). While most companies have not developed a clear roadmap, more than a quarter of financial services organizations (27%) say they have a multiyear plan with defined milestones and goals. Only 21% of nonfinancial services organizations have programs mapped out.

The TPRM programs of companies in financial services industries are more likely to be internally aligned across other parts of the business. Two-thirds of financial services organizations identify and monitor external events by coordinating with an internal department.

However, organizations with mature TPRM programs must not get complacent and should be sure to examine the complete picture around all facets of risk. "Financial services are way ahead, but very often, they are looking only at the cyber risk, compliance and anti-money laundering — and not always considering other risk domains, such as ESG," says Netta Nyholm, EY Europe, Middle East, India and Africa (EMEIA-Germany) Third Party Risk Leader (Non-FSO).

27%

of financial services organizations have a multiyear TPRM plan with defined milestones and goals

VS.

21%

of nonfinancial services

2 Centralized TPRM has clear advantages

In all, 90% of organizations are moving toward centralized risk management, up from 85% in our survey from the prior year. Among those surveyed, 54% of organizations use centralized risk management (down 6% from 2021), 36% use a hybrid approach (up 11% from 2021), and 10% use a decentralized program (compared with 12% in 2021).

90%

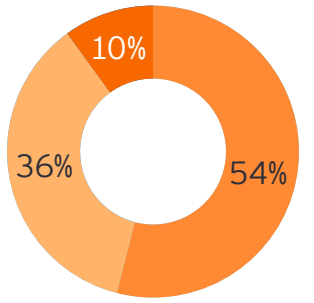
of organizations are moving toward centralized risk management

Centralizing TPRM allows an organization to assess its third-party risk as a whole, apply consistency, prioritize risk and plan to make optimal use of resources to manage or mitigate risk. We also see organizations, particularly global organizations with multiple regulators, adopt a hybrid approach, using both co-source and managed service arrangements, and internal teams based on location to maintain specialized knowledge in each region. However, whatever the operating model, the risk ownership and decision-making always remain in-house.

"Organizations that are ahead of the markets have understood the value of combined business areas working together," Nyholm says. "Many have reached a level where they understand that there's not going to be one owner, but a governance team or committee of people, depending on the risk. They are looking at it from different risk lenses, but they can only gain the true benefit for the company if they are working collaboratively."

Only 10% of respondents report that they will continue to operate in a decentralized manner, assessing third parties separately or in risk silos. However, this increases the likelihood of duplicating efforts or failing to capitalize on efficiencies.

Q **Which of the following best describes the structure of your TPRM program?**



- Centralized
- Hybrid (+11% from 2021)
- Decentralized

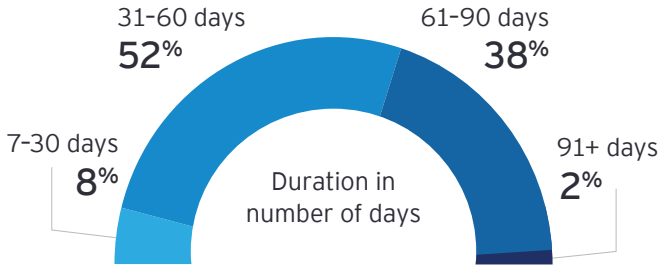
Business benefits of centralized TPRM

Organizations with centralized TPRM structures manage almost twice as many third parties effectively as their counterparts with hybrid TPRM structures. They have a better understanding of the correlating risks and a better understanding of the mitigating measures. They are also more likely to have a general risk management team and TPRM team responsible for ongoing monitoring of third parties.

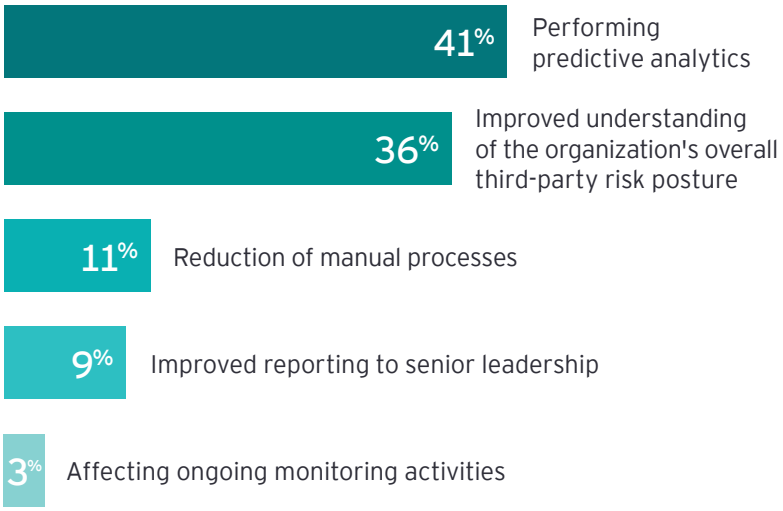
Organizations with a centralized model are able to perform control assessments faster: 64% of those with centralized risk structures can perform control assessments in 31 to 60 days. Only 43% of organizations with hybrid structures are able to say the same. For organizations with a hybrid model, about half say they are completing their assessments in 61 to 90 days.

Respondents with centralized TPRM are realizing value from their technology investments. More than half report that embedding technology into their organization helps them with performing predictive analytics.

Q **Approximately how long does it take your organization to perform control assessments of third parties?**



Q **How does embedding technology or tools and data into your organization best enable the overall process of risk reporting?**

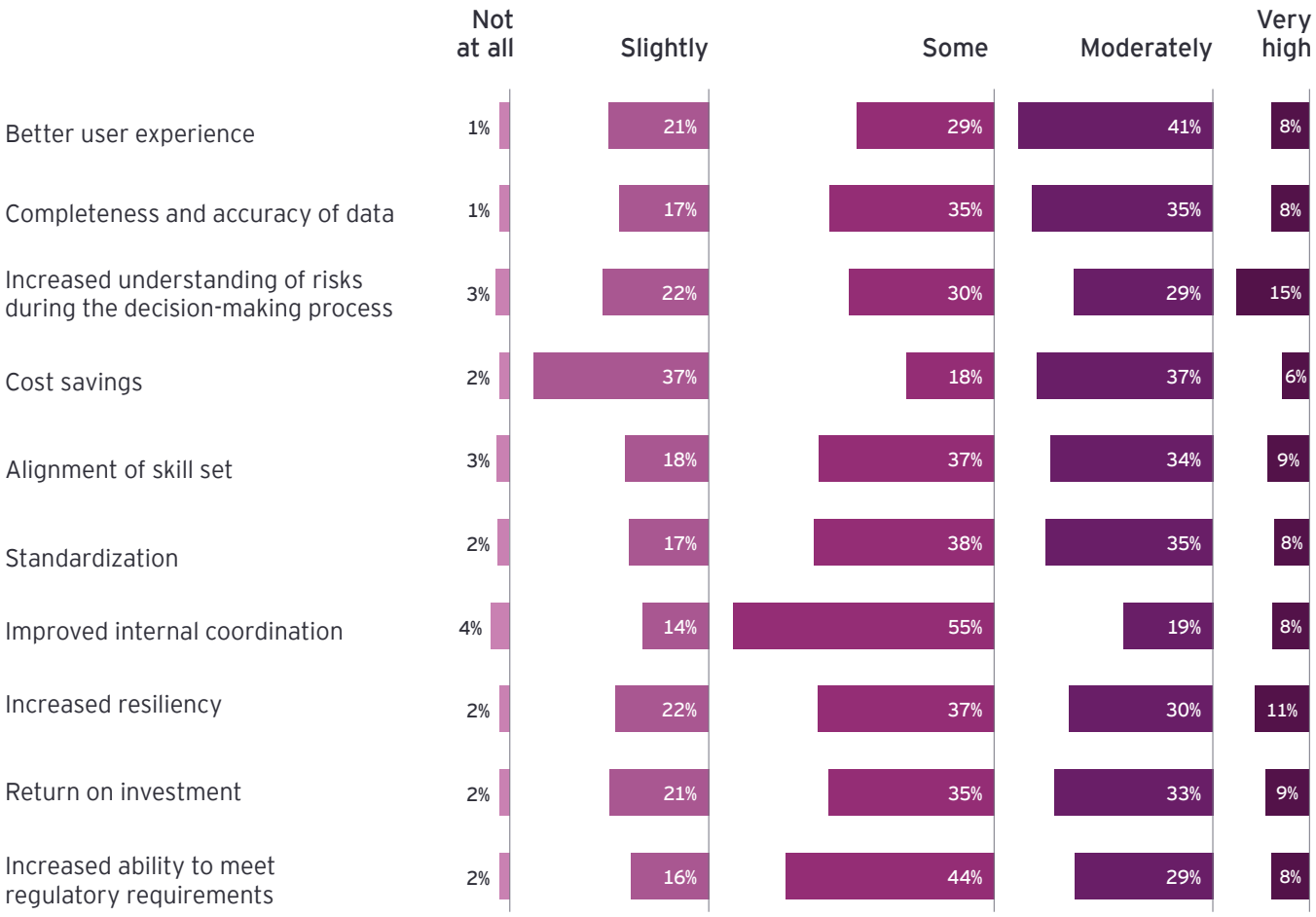


Firms that have created business cases for their TPRM programs have realized significant indirect benefits for the overall effectiveness of their programs beyond solely a reduction in their costs.

They reported the following benefits:

- A better user experience (49%)
- More complete and accurate data (45%)
- Increased understanding of risks during the decision-making process (44%)
- Cost savings (43%)
- Alignment of skill sets (43%)
- Standardization (43%)
- Improved internal coordination (27%)

Q To what extent have you seen the following benefits from the maturation of your TPRM program?

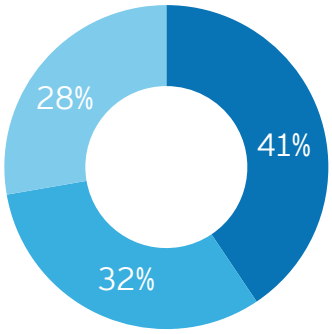


> Organizations that are ahead of the markets have understood the value of combined business areas working together. Many have reached a level where they understand that there's not going to be one owner, but a governance team or committee of people, depending on the risk. They are looking at it from different risk lenses, but they can only gain the true benefit for the company if they are working collaboratively.

Netta Nyholm
EY Europe, Middle East, India and Africa (EMEIA-Germany) Third Party Risk Leader (Non-FSO)

3 Benefits along the stages of program maturity

Q **How long has your organization's TPRM program been operational?**



- Between three and five years
- More than five years
- Less than three years

Third-party risk management has grown from a compliance exercise to a strategic tool for business. But while organizations realize the benefits, establishing and developing an effective TPRM program poses challenges.

Less than one-third of survey participants have run a TPRM program for longer than five years. Some organizations only invest in their programs after they experience a breach or failure, and there are other organizations that do not monitor their third parties with any true discipline. Among those that do, outside of the largest global organizations, many organizations are still using spreadsheets and time-consuming manual processes to track third parties. While spreadsheet-based applications are highly functional, they are limited, and cloud-based software is ideal.

"Organizations are trying to move away from Excel. They realized they need more real-time, on-demand reporting and not just a yearly assessment or semi-annual report," says Harald deRopp, Asia-Pacific (Japan) Third Party Risk Leader. "But it's a slow process."

Organizations that have assessed their network of third parties and their organization's risk from a central viewpoint are headed in the right direction. Beyond that, more mature organizations are developing a common taxonomy across internal and external sources and using advanced software that can be filtered for real-time processing, greater transparency and facilitating decision-making.

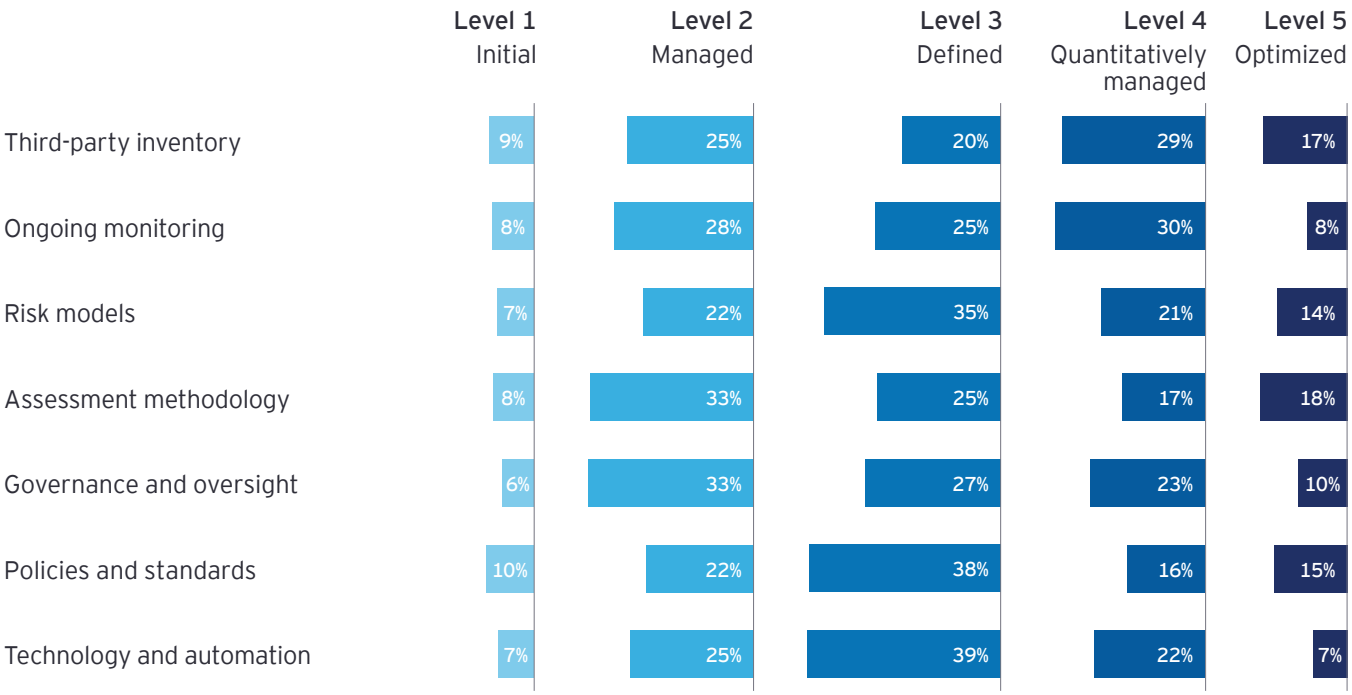
Stages of maturity

New: Less than two years
New programs could use their age to their advantage. Starting a TPRM program today puts them in a position to not only use the most recent technology, like artificial intelligence and machine learning, but rely on the ones that have been tried and tested.

Developing: Three to five years
Organizations with developing TPRM programs report they have a high return on investment from their TPRM maturation. More than half are expecting cost savings.

Mature: Five or more years
Mature organizations are more likely to have their processes standardized across the organization and are more likely to follow leading practices. For example, they escalate and align to enterprise risk processes when third parties do not respond to questionnaires. Sixty-three percent send one aggregated questionnaire to their third parties rather than multiple. Mature organizations also invest more in data capabilities.

Q **What level of maturity do you feel your TPRM program has achieved across the seven foundational components?**



Level 1: Initial
Processes unpredictable, poorly controlled and reactive

Level 2: Managed
Processes customized for projects and often reactive

Level 3: Defined
Processes customized for the organization and proactive

Level 4: Quantitatively managed
Processes measured and controlled

Level 5: Optimized
Focused on process improvement

4 Organizations are integrating environmental, social and governance risk

Environmental, social and governance (ESG) commitments are a growing priority in third-party risk management. Companies have made public commitments, and stakeholders — from boards to customers — will hold them accountable.

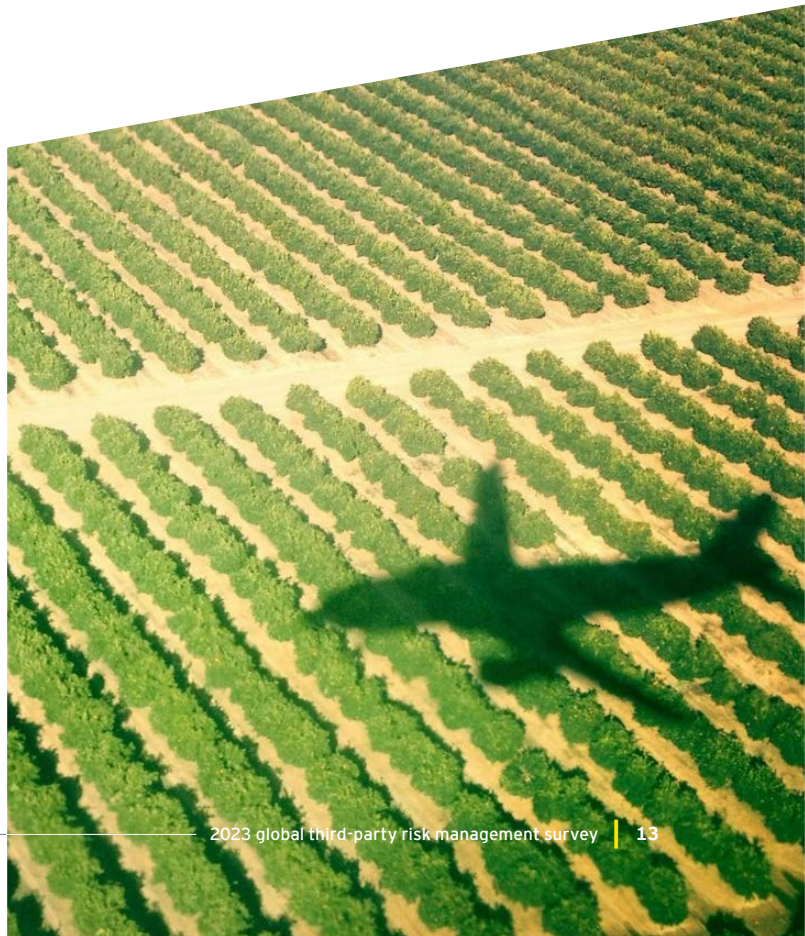
The top external commitments companies made for 2023 are in diversity, equity and inclusion (30%) and climate change and GHG emission (28%).

Most organizations (54%) include ESG in risk inventory reporting. Their top priorities include compliance with local regulations, corporate responsibility and stakeholder expectations. Nearly one-third (32%) include clauses requiring third parties to comply with their own ESG policies and regulations.

"In order for organizations to have a robust ESG program, their ESG commitments need to extend into their third parties as well," says Michael Giarrusso, EY Americas FSO Third Party Risk Leader. "They need to make sure that they are performing proper due diligence against their third parties to confirm that they are in line with their own strategic goals from a sustainability and social justice perspective."

ESG commitments need to extend into third parties:

- Are the workers treated fairly and compensated fairly?
- Is the organization investing in or dedicating resources to helping communities and community outreach?
- Do the third parties have travel policies to track emissions and carbon footprint?
- Do they have their own environmental commitments?
- Organizations with newer third-party risk management programs and those with hybrid TPRM are more likely to integrate ESG into their strategy and processes.



ESG risk conversations are evolving

Third-party ESG risk management is a developing area of risk management, and 47% of organizations consider ESG a separate risk domain. These developments are causing organizations to reexamine how they set their priorities, which commitments they publicly make and how they spend their resources, efforts and investments.

"Organizations are facing challenges with their identity — not only what they want to represent as a company, but also how they want to measure, monitor, track and report against that commitment," says Chris Watson, EY Americas Risk and Supplier Services Leader. "Talking about what we care about in this way causes a lot of conflicting views that can be very challenging for a complex organization."

Executives in financial services industries cite their top ESG priorities as compliance with local regulations and stakeholder expectations and requirements, whereas those in nonfinancial services industries cite corporate responsibility and diversity, equity and inclusion:

- **Forty-five percent** of survey respondents are increasing the diversity of their suppliers to meet ESG goals.
- **Twenty-three percent** said if a key supplier did not meet their ESG requirements, they would stop working with that supplier.

Despite their differing priorities, about two-thirds of respondents across industries experience the same pain points for meeting ESG goals: a lack of coordination between internal stakeholders and third-party risk management.

Which of these tools or technologies are you planning to integrate into the ESG function to better manage risk over the next two years?

Select all that apply.

39%	Automation
34%	Data analytics
24%	External data providers
21%	Artificial intelligence
21%	Machine learning

What are the top ESG priorities or risks currently faced by your organization's TPRM program?

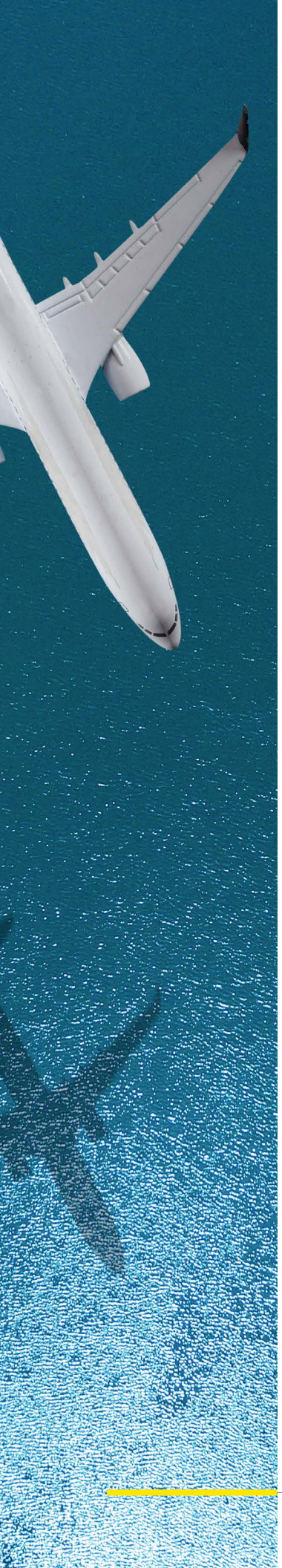
Select all that apply.

38%	Compliance with local regulations
38%	Corporate responsibility
35%	Stakeholder expectations or requirements
33%	Diversity, equity and inclusion
31%	Regard for reputational risk with clients and customers
29%	Sustainable finance and investments
27%	Health, safety and wellbeing
23%	Climate change and energy and GHG emission
22%	Ethics and board accountability
22%	Sustainable buildings
20%	Waste, water or biodiversity
15%	Human rights (15%) e.g., trafficking, modern slavery

Which of these tools or technologies are you planning to integrate into the ESG function to better manage risk over the next two years?

Select all that apply.

54%	Our risk inventory reporting includes ESG risks
45%	We are increasing the diversity of our suppliers to meet ESG goals e.g., minority-owned businesses
32%	Our contracts include clauses requiring third parties to comply with our company's ESG policies or regulations
23%	If a key supplier did not meet our ESG requirements, we would stop working with that supplier
16%	We have specific targets to reduce our supply chain emissions that we apply in our contracts
7%	We have set a certain amount of managed spend to be used with vendors officially certified as diverse



> Having a strong third-party program can support resiliency, but it needs to be intentional. Make sure that you're identifying those third parties that are supporting critical business processes, and then have plans in place — whether it's contingency or exit strategies — for those third parties in the event of a business disruption.

Michael Giarrusso
EY Americas FSO Third Party Risk Leader

5 Resiliency and third-party risk management

Q **Which of the following actions do you take as part of your business resiliency plan for critical third parties?**

Select all that apply.

51%
Maintain an integrated resiliency plan

47%
Conduct integrated resiliency testing

45%
Perform scenario analysis

45%
Maintain exit strategies or contingency plans

40%
Test exit strategies, contingency plans and business continuity plans

As companies focus on their own resiliency, the resiliency of their third parties is a higher priority. Today, organizations do more due diligence (most ask more than 100 questions on their control assessments) and plan for when things go wrong.

Nearly half (48%) of organizations have exit strategies or contingency plans for high-risk third parties, which means that more than half are unprepared.

Companies are building resilience by maintaining an integrated resiliency plan, conducting internal resiliency testing and performing scenario analysis, exit strategies, contingency plans and business continuity plans:

- **Fifty-one percent** of organizations maintain an integrated resiliency plan for critical third parties, **47%** conduct integrated resiliency testing, and **45%** perform scenario analysis.

Banking and capital markets tend to have a more mature approach to TPRM, which helped with resiliency during the early stages of the pandemic when many people were worried about business disruption as third parties were unable to staff and deliver the services needed, Giarrusso observes. The more mature organizations that had a very strong third-party program were able to quickly identify their most important third parties and then assess their comfort level with the third party's ability to continue to provide services uninterrupted.

As a service provider to the economy and to customers, banks need to make sure they're resilient and that people have access to their financial services needs. "To the extent that third parties are supporting those critical processes, it's very important that they're monitoring their resilience," Giarrusso says. "Having a strong third-party program can support resiliency, but it needs to be intentional. Make sure that you're identifying those third parties that are supporting critical business processes and then have plans in place — whether it's contingency or exit strategies — for those third parties in the event of a business disruption."

77%

of organizations send between 101 and 350 questions on third-party control assessments

6 Major shifts in TPRM over the past three years

1. Shift to centralization

We've seen movement toward centralized, organization-wide standards for third-party risk management programs and additional due diligence around third-party risk that includes a governance or reporting component.

The most mature organizations tend to be moving to include all third-party types into a single program rather than assessing them separately.

2. Shift to using external resources for TPRM planning

Continuing a trend from the 2020 EY TPRM Survey, TPRM programs increasingly rely on co-sourcing and managed services arrangements to help reduce cost, drive efficiencies, solve skill set gaps and give them flexibility as demand varies. And organizations are seeking smarter ways to understand risk by using external resources.

"As the scale of these programs has exponentially grown, we're seeing this huge trend of organizations looking at external data sources, either using them up front to help the inherent risk tiering or as part of their ongoing continuous monitoring for their critical third parties," Kelly says. "They're looking at using external data sources to start managing their fourth parties as well."

The survey noted:

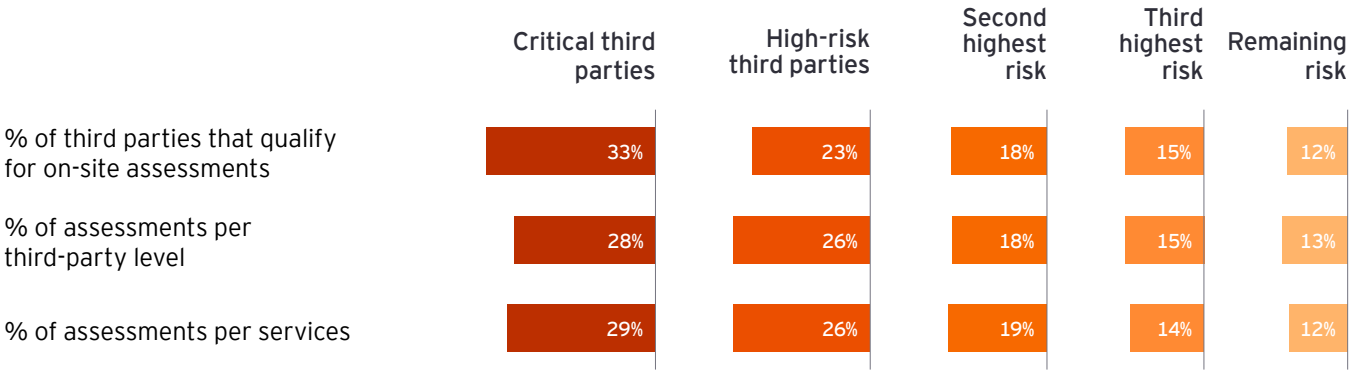
- **Fifty-four percent** of organizations identify, assess and monitor subcontractor (e.g., fourth, fifth and nth party) relationships through third-party diligence.
- **Forty-four percent** of organizations expect to use managed service providers more in the next two to three years, while 59% plan to use more co-sourced arrangements.

44%

of organizations expect to use managed service providers more in the next two to three years

Q **Of the total third parties, what share are classified in the following areas?**

Select all that apply.



3. Risk tiering

Organizations continue to zero in on critical third parties while adding further oversight and controls. Many organizations use financial impact and criticality as the most important criteria to define a critical third party, followed by sensitivity of the type of data and systems accessed and sensitivity of data involved. Critical parties are separated for additional monitoring activities. Executives report that the most difficult challenge when reporting risk in third-party risk inventories is from assessing the effects of unexpected external events.

4. Increased use of data and technology

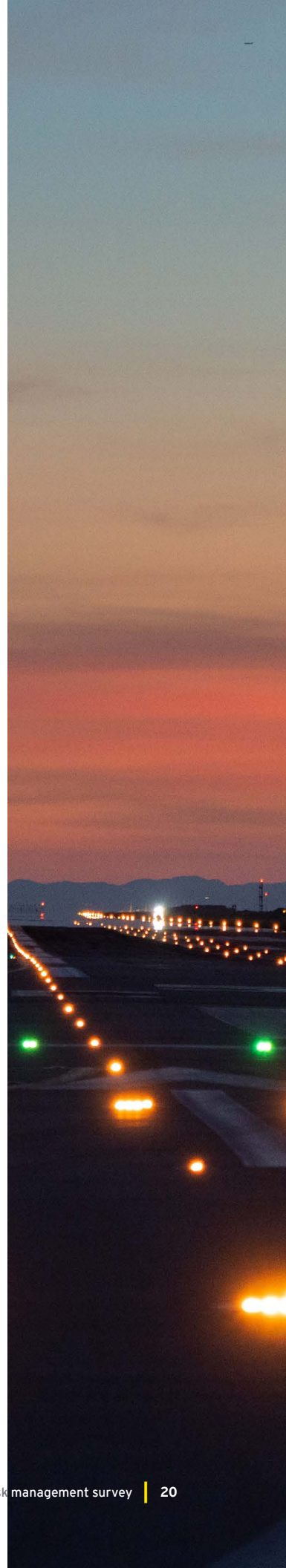
Embedding technology, automation and external data into their risk reporting process has improved several aspects of TPRM for respondents. Thirty-six percent report improved understanding of their overall third-party risk posture:

- **Forty-two percent** of organizations plan to integrate automation to better manage reporting.
- **Sixty-three percent** of organizations plan to integrate external data providers and automation to better manage inherent risk assessments in the next 2–3 years.

“

The only way to completely zero out your third-party risk is to not work with third parties, but that’s not going to happen. So it’s more about, ‘How do you identify, manage and mitigate?’ We’re moving from the era of just identification into management and mitigation.

Joseph Kelly
EY Oceania Third Party Risk Leader



7 Leading practices for third-party risk

Define objectives and scope
To build a successful TPRM program and operational resilience, organizations should consider aligning their plans to an existing operational resilience framework, such as the Digital Operational Resilience Act, NIS2 Directive and the UK Operational Resilience Framework. These frameworks set criteria and expectations for cybersecurity, information technology, third-party dependency management and business continuity planning and testing. Perform an impact assessment and gap analysis against the currently proposed drafts.

Fully understand, document and maintain your third-party inventory

Develop policies and procedures
Lack of coordination between internal stakeholders was cited as the biggest pain point for organizations.

Enhance ongoing monitoring
While initial due diligence is vital, more robust ongoing monitoring of third parties enables more dynamic risk reporting.

Establish a governance structure
Regardless of ownership, TPRM requires input from multiple functions and teams, making well-defined governance crucial. It is recommended to have a consistent global policy with local addendums for multi-jurisdictional organizations.

Implement technology and automation
TPRM programs that integrate automation and external data providers into the supplier lifecycle and embed cross-functional workflows, e.g., procurement, cyber risk, resiliency, are more effective in managing third-party risk and reporting to senior leadership.

Streamline customer experience
Fifty-four percent of organizations send one aggregated or centralized questionnaire, while 46% send multiple questionnaires from different risk domains. Forty-nine percent of organizations are in the process of developing a strategy to improve the customer response function.

Conclusion

Third-party risk management increases resiliency and has the potential to become a strategic tool for businesses. While organizations are aware of the advantages, establishing and developing an effective TPRM program presents difficulties.

Leading organizations are making efforts to advance their TPRM programs by attempting to get a better picture of overall third-party risk, tiering risk according to critical needs and adding more TPRM reporting and resourcing capabilities beyond spreadsheets. To increase efficiency and enable more strategic risk management decisions, organizations are evaluating emerging risks and impacts on their third parties and risk governance and are continuing to use centralized and hybrid risk management programs.

Contacts

Americas

Michael Giarrusso
EY Americas FSO
Third Party Risk Leader
michael.giarrusso@ey.com
+1 617 585 0395

Scott McCowan
EY Americas
Risk Management Leader
scott.mccowan@ey.com
+1 617 585 3487

Chris Watson
EY Americas
Risk and Supplier Services Leader
christopher.watson@ey.com
+1 614 297 3215

Asia-Pacific

Harald deRopp
Asia-Pacific (Japan)
Third Party Risk Leader
harald.deropp@jp.ey.com
+81 3 3503 1110

Joseph Kelly
EY Oceania
Third Party Risk Leader
joseph.kelly@au.ey.com
+61 400 953 895

Europe, Middle East, India and Africa (EMEIA)

Netta Nyholm
EY Europe, Middle East,
India and Africa (EMEIA-Germany)
Third Party Risk Leader (Non-FSO)
netta.nyholm@de.ey.com
+49 160 9391 6427

Kanika Seth
EY Global Financial Services
Third Party Risk Leader
kseth@uk.ey.com
+44 20 7951 7469

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

CSG no. 2301-4172621

EYG no. 004506-23Gbl
ED None

ey.com