Building trust with your third parties in a technology-driven and disruptive world

EY global third-party risk management survey highlights 2019–20

Building a better working world

> TPRM programs today need to be more than agile and cost-effective. They must also help organizations be resilient through quick identification and management of risks during a crisis.

Vignesh Veerasamy
EY Global and Americas TPRM Leader

> As the structure and maturity of third-party risk functions continue to evolve, it has never been more important to maintain strong governance routines.

Matthew Moog
EY Global Third-Party Risk Leader in Financial Services

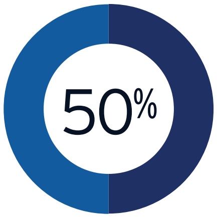
Contents

Key takeaways

EY global third-party risk management survey highlights

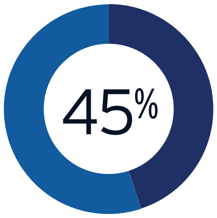
In the summer and fall of 2019, EY surveyed 246 global institutions that had a third-party risk management (TPRM) function in various sectors, including but not limited to, retail and commercial banking, investment banking, insurance, advanced manufacturing and mobility, technology, media and entertainment, power and utilities, and health.

Operating model



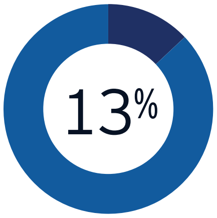
of organizations reported having a centralized structure.

Execution



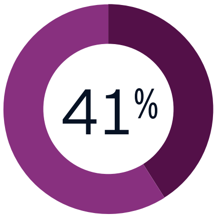
of organizations expect to use more of managed services to execute their TPRM program/function in two to three years.

Resourcing model



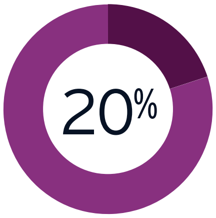
of resources, on average, are dedicated to supporting the TPRM program/function.

Tools and technology



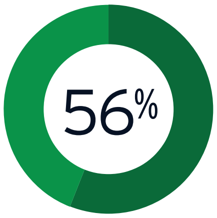
of organizations have a TPRM technology platform. More than half of those have links to external threat intelligence data or supplier data.

Innovation



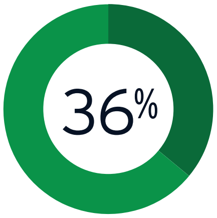
of organizations currently used advanced analytics and more expect to use it in two to three years.

Fourth-party management



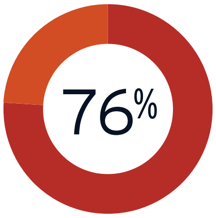
of organizations rely on the contractual terms established with the third party or third party's assessment to assess/monitor fourth parties.

Cybersecurity



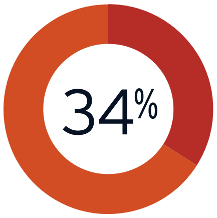
of organizations had a data breach caused by a third party over the past two years.

Assessments



of organizations reassess (risk/control assessment) critical third parties on an annual basis.

Inherent risk



of organizations refresh inherent risk profiles of third parties based upon their inherent rating.

The EY third-party risk management survey aims to give organizations a perspective on trends in how organizations manage, monitor and magnify TPRM functions.

The survey covers a broad range of organizations, including advanced manufacturing and mobility, financial services, banking and capital markets, consumer, health, insurance, life sciences, power and utilities, technology, media and entertainment, and telecommunications.

The rapidly evolving threat around the COVID-19 virus is raising concerns about the resilience of enterprises globally. One potentially overlooked vulnerability? The increasing dependence on third parties. The interconnectedness of today's business environment and the use of external vendors – from supply chains to the delivery of critical business services – poses a risk of disruption that can result in significant revenue loss.

For this reason, our TPRM survey is timely and identifies some notable trends in the following five areas:

1. **Operating model and governance**
2. **Automation, technology and reporting**
3. **Fourth parties, data breaches and resiliency**
4. **Risk expansion and frameworks**
5. **Emerging focus areas**

These trends include a gradual movement toward centralization of risk in parallel with the increased use of consortia/market utilities to expand the coverage and depth of due diligence. While technologies such as artificial intelligence (AI) are increasing in use, organizations should define their own specific reporting framework and requirements before automating risk-related processes.

There are also heightened expectations from stakeholders and a growing awareness of the risks presented by entering new ventures and markets with respect to partners, joint ventures, collaborators, fourth parties and other relationship structures. These fourth parties remain a blind spot for the vast majority of organizations.

1 Operating model and governance

There is still no consensus in the industry around the ownership of TPRM programs. However, we are seeing a continued gradual movement toward centralization.

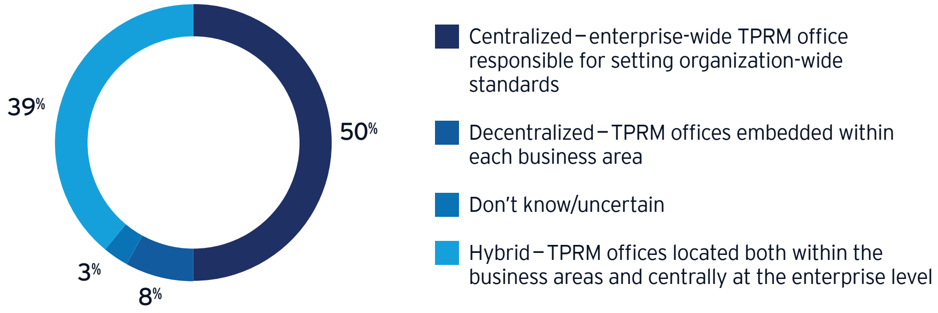
There are numerous reasons for this: the need to consider various risk lenses (for example, privacy, fourth-party risk, resiliency) in a consistent manner; having an end-to-end transparent view into the third-party engagement life cycle; a clear delineation of responsibility and accountability across the lines of defense; and making adherence to policies and standards more rigorous and consistent.

There is also pressure to deliver due diligence outcomes faster, across a broader and deeper scope. To do this, organizations are turning to market utilities more often to decrease cycle times and increase the quality of data going into due diligence and ongoing oversight decisions. At the same time, organizations are shifting the internal headcount that traditionally supported these functions to more value-adding risk management activities, and engaging external parties to handle the variable nature of assessment volumes.

Q How is your third-party risk management program/function structured?

Third-party risk management program/function organization, governance and oversight

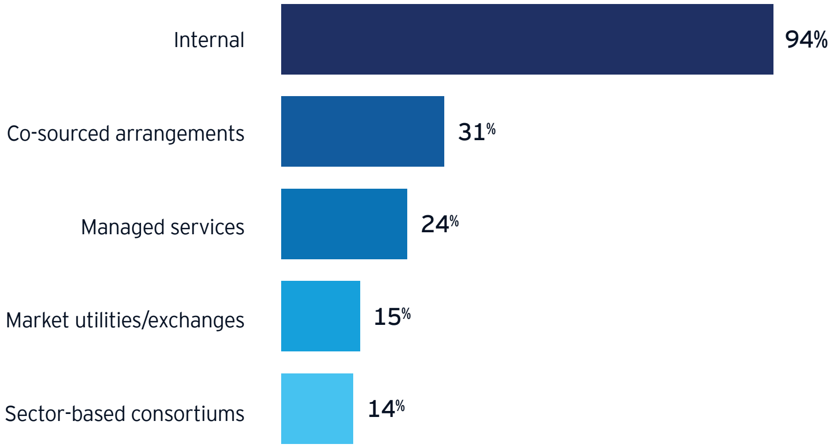
Centralized and hybrid models continue to be the most common structure for TPRM programs, signifying the importance of a consistent, yet flexible, TPRM function across the organization.



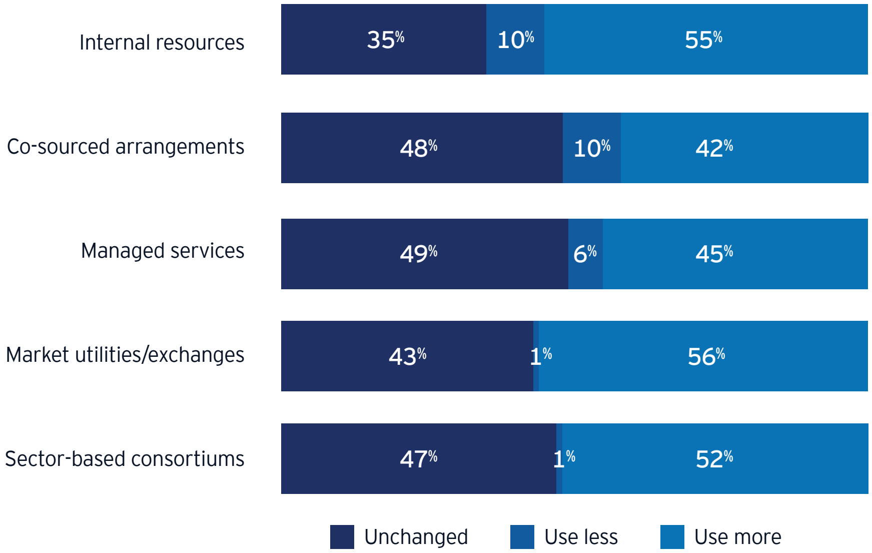
TPRM execution

Looking out over the next two to three years, there is a clear desire among the organizations surveyed to leverage external solutions more actively. More than 40% of the organizations surveyed expect to more frequently use managed service providers or co-sourcing to execute their third-party risk management function; that figure jumps to more than 50% for market utilities or sector-based consortiums.

Q Does your organization currently use any of the following for the execution of your third-party risk management program/function?



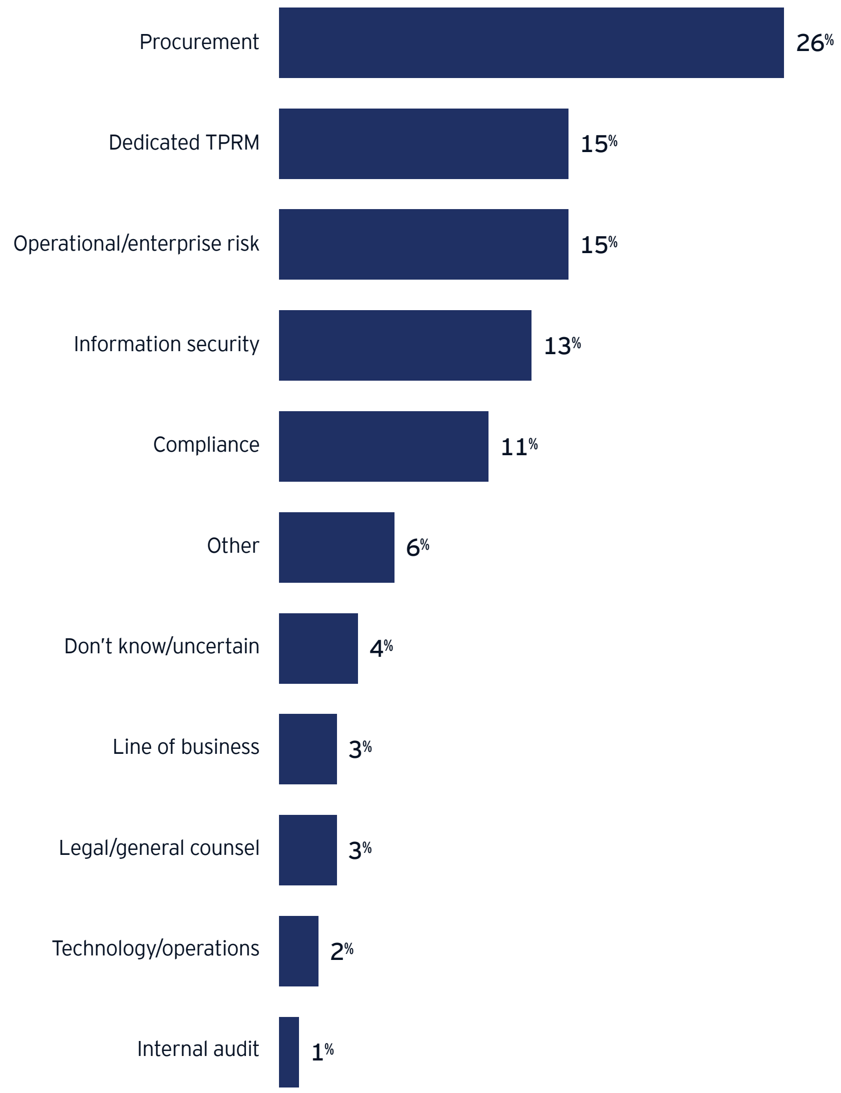
Q How do you expect that to change in the next two to three years?



Q What area has primary ownership of the third-party risk management program/function?

Integrated with TPRM program

There is still no consensus across the organizations surveyed as to who owns the TPRM function; 26% of respondents indicated that procurement has primary ownership, while 15% indicated that operational/enterprise risk owns it. An additional 15% indicated they have a dedicated TPRM group that owns it.



2 Automation, technology and reporting

Over the last few years, organizations have moved toward streamlining and integrating technology and various toolsets across the third-party management ecosystem.

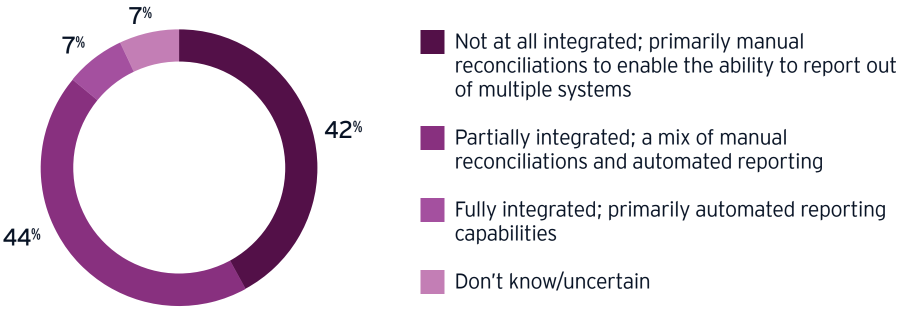
Clients have shown interest and have started conversations about leveraging advanced analytics and AI to demonstrate the value of TPRM programs, find opportunities to manage costs, and identify better insights in data to respond to complex new regulatory requirements. However, only one in five organizations surveyed are currently using advanced analytics. Organizations are also seeking integration with consortia, market utilities and other management services.

However, tech-based tools are not a cure-all. Organizations should define reporting frameworks and requirements (key performance and risk indicators) that are fit for purpose and unique to the organization before enabling them through technology. As organizations leverage technology and automation, they have an opportunity to gather more data across many processes to improve reporting, TPRM and procurement processes and analytics.

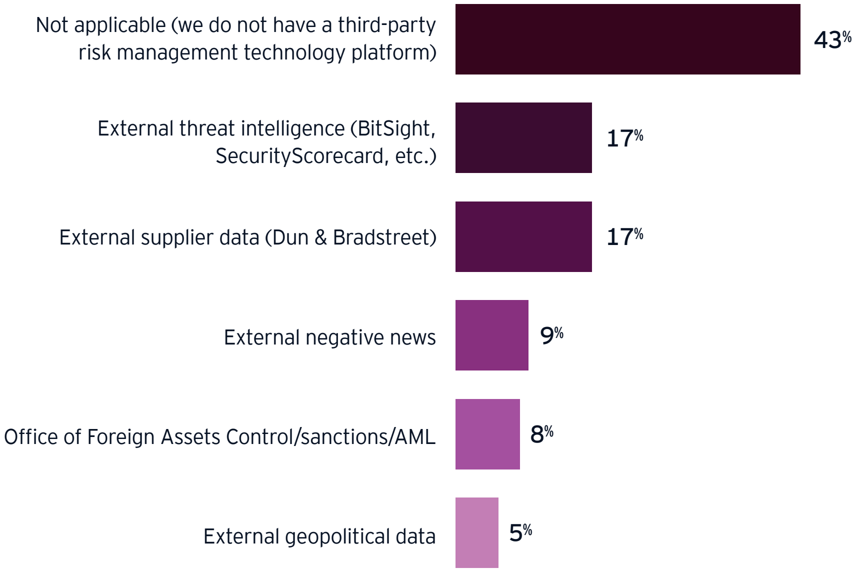
Technology

Among the surveyed organizations that use tools/technology as part of their TPRM programs, few note that a technology platform is fully integrated within the organization. Of the organizations that do have a technology platform, they are actively incorporating external data into their systems via application program interfaces (APIs). There is an opportunity for technology integration and platform adoption to enhance today's predominantly manual processes across TPRM.

Q How well integrated are the various tools your organization uses as part of your third-party risk management program/ function?



Q If you have a third-party risk management technology platform, which active application program interfaces are configured to feed your third-party risk management technology platform to support ongoing monitoring activities?

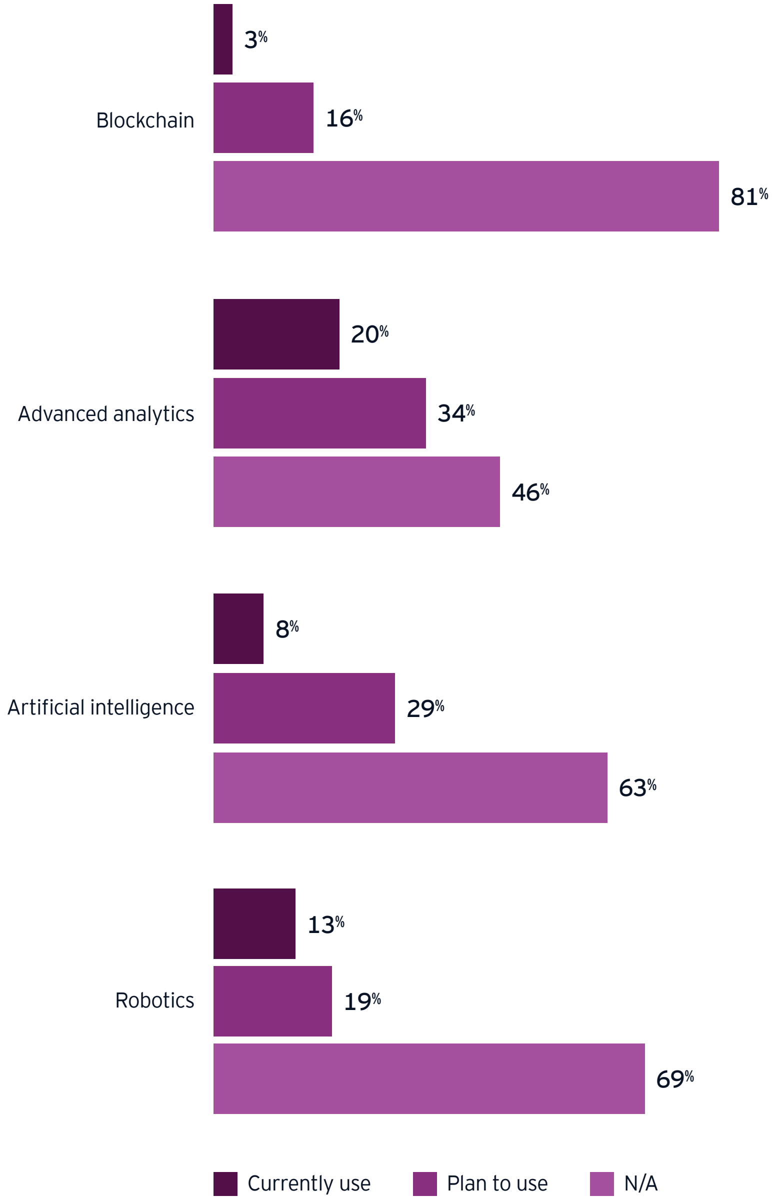


Q A. Does your organization currently use any of the following emerging technologies to support your third-party risk management program/function?

B. If not, does your organization plan to begin using any of the following in the next two to three years?

Innovation

Just one in five organizations surveyed are using advanced analytics, and even fewer are using AI, robotics or blockchain. However, many more organizations recognize the benefits that such technology can provide. More than one in three expect to start using advanced analytics in the next two to three years, and almost one in three plan to use AI.



3 Fourth parties, data breaches and resiliency

Fourth parties remain a blind spot for many organizations. Relatively few organizations perform their own independent reviews of fourth parties and are increasingly relying on contractual terms between the third and fourth party for oversight.

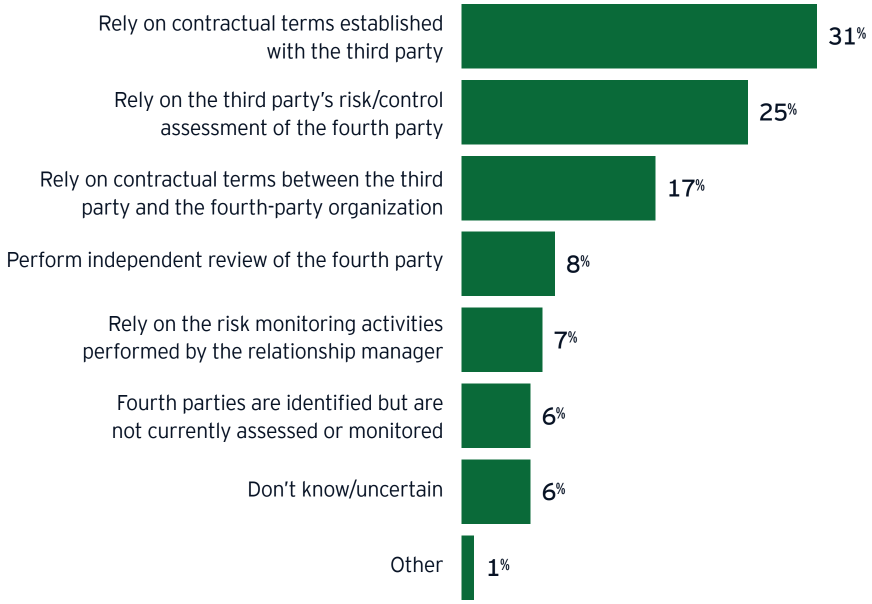
Fourth-party reviews should be higher on the risk management agenda as they can present a blind spot for various third-party risks to the organization. The organization, as data owners, will ultimately be held accountable for any nth (fourth, fifth, sixth) party breach. The organization must always know where its data is going, especially customer data, how it is being handled or used and who is accessing and/or using the data.

Organizations can reduce their potential exposure by evaluating risks up front and considering fourth parties within the inherent risk assessment at the initial contracting, onboarding phase or within ongoing oversight activities. They could also leverage automated threat intelligence tools for more insightful reviews of fourth parties; this is an approach that the majority of survey respondents do not use today.

Q How does your organization assess/monitor fourth parties?

Fourth-party monitoring

A meaningfully larger proportion of the organizations surveyed rely on contractual terms with their third parties for the purposes of overseeing/monitoring fourth parties. Increasingly, firms are also relying on contractual terms between the third and fourth party. Relatively few of the surveyed organizations (less than 20%) perform their own independent reviews of fourth parties.

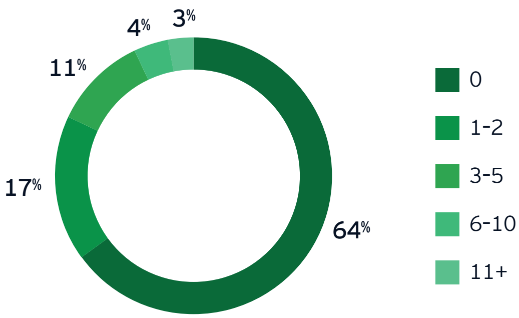


Cybersecurity and threat intelligence

A significant number of the organizations surveyed have faced breaches or outages caused by third parties. Almost one in five organizations reported having at least three breaches, while nearly in one in three reported at least three outages.

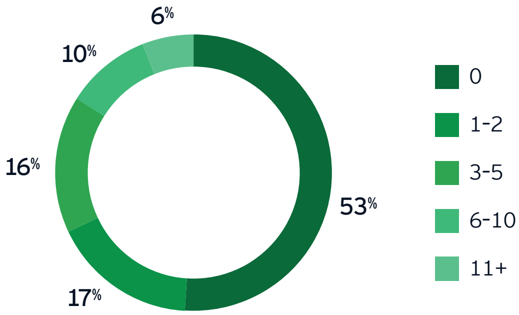
Q Over the past two years, how many data breaches or losses have been caused by third parties?

Data breaches caused by third parties



Q Over the past two years, how many outages have been caused by third parties?

Outages caused by third parties



4 Risk expansion and frameworks

The organizations surveyed generally rely on standardized frameworks as a baseline for their risk assessment questionnaires, though the specific frameworks they use vary widely.

Frameworks for other risk lenses are newly developed (for example, General Data Privacy Regulation and California Consumer Privacy Act) or may not exist at all, as organizations do not have a reference point on what others are using to address these risks. This may be why more organizations are looking to leverage external data sources, to understand and evaluate their risk expansion and to better align their TPRM methodology.

Risk expansions of regulatory compliance and operational risks are prevalent. Some organizations are actually weighing the cost and effort of compliance against the likelihood of enforcement actions against them.

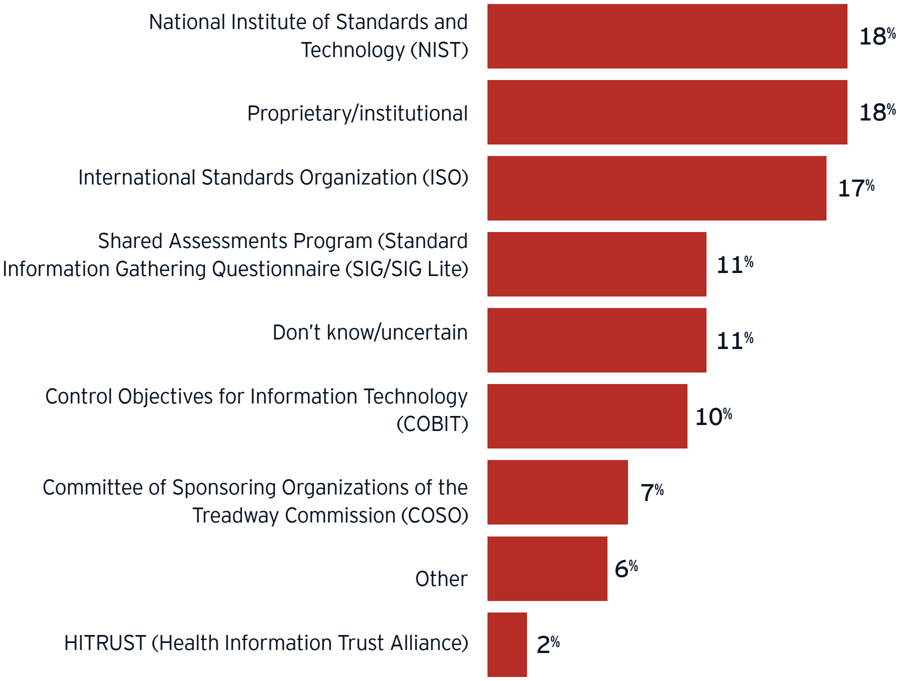
If a company is expanding, only limited frameworks are available to allow for simultaneous assessment of third parties in cybersecurity and privacy, as well as the other risk expansion areas like resiliency.

Assessments

Over the past two to three years, there has been a significant uptick in the proportion of firms using NIST, although ISO and COBIT have also seen increased usage by organizations. By using industry-proven and trusted frameworks such as NIST, the organizations surveyed feel comfortable with using such frameworks as a baseline.

Q Which framework is used as a baseline for your risk assessment questionnaire?

Risk assessment questionnaire framework

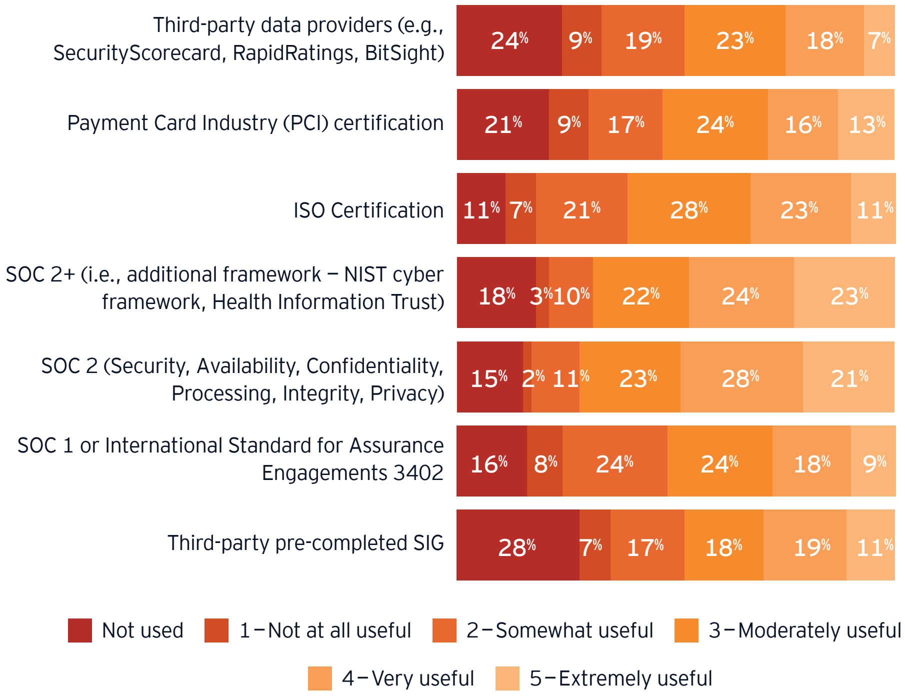


Assessments

About half of the organizations surveyed found System and Organization Controls (SOC) 2 or SOC 2+ an additional framework to be useful, consistent with previous results. Other frameworks (ISO, PCI, etc.) are seen to be moderately less useful; however, organizations still have not found any frameworks that have been entirely successful in reducing or eliminating the need to perform a risk/control assessment.

Q On a 5-point scale, with 1 being not at all useful and 5 being extremely useful, how useful is each of the following in reducing or removing the need to perform a risk/control assessment on a third party?

Usefulness of tools/documentation in reducing/removing risk



5 Emerging focus areas

Organizations are faced with heightened expectations from risk management stakeholders, as well as entry into new ventures and markets, which carry their own risks.

There has also been enhanced focus and dialogue in other areas, including cybersecurity, fourth-party and supply chain risk, and global coverage and applicability of regulations.

Additionally, there is a growing focus on the definition of critical relationships, especially at the board level. While the demand for oversight of TPRM programs increases, there is also more integration of TPRM with Operational Risk and Enterprise Risk Management programs to provide a composite view to management. Organizations have a desire for more board involvement, but at the moment, the reality is quite different.

Q During your organization's most recent regulatory body review and most recent internal audit of your third-party risk management program/function, what were the two to three most important areas of focus? Please select no more than three.

Regulatory and internal audit exams

As with previous years, oversight and governance was the dominant area of focus among the organizations surveyed, with cybersecurity following in both areas and enterprise-critical third parties following for regulatory body and onboarding activities following for internal audit.

Important areas of focus	Regulatory body review	Internal audit
Oversight and governance	72	94
Cybersecurity	45	56
Enterprise-critical third parties	33	27
Third-party assessments – information security and business continuity	29	36
Inherent risk assessment	25	39
Fourth-party oversight and governance	16	7
Privacy/confidentiality	16	23
Issue management and/or risk acceptance	15	29
Onboarding activities	14	45
Third-party assessments – compliance	13	25
Operating models	12	19
Maintenance of third-party inventory	10	23
Foreign-based third parties	8	6
Nontraditional third parties (i.e., brokers, agents, financial intermediaries)	7	3
Third-party assessments – performance	4	12
Consumer protection/compliance	4	3
Residual risk model	3	10
Other	3	4
Not applicable	52	39

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYG no. 002940-20Gbl
2004-3465938
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts

GLOBAL

Amy Brachio
EY Global Advisory Risk &
Performance Improvement Leader
amy.brachio@ey.com
+1 612 371 8537

Nitin Bhatt
EY Global Advisory Risk
Transformation Leader
nitin.bhatt@in.ey.com
+91 80 6727 5127

AMERICAS

Matthew Moog
EY Global Third-Party Risk Leader in
Financial Services
matthew.moog@ey.com
+1 201 551 5030

Vignesh Veerasamy
EY Global and Americas
TPRM Leader
vignesh.veerasamy@ey.com
+1 415 894 8708

Michael Giarrusso
Americas TPRM Financial Services
Leader
michael.giarrusso@ey.com
+1 617 585 0395

ASIA-PACIFIC

Chris Lim
APAC Financial
Services Organization
Risk Transformation Leader
chris.lim@sg.ey.com
+65 6309 6320

Steven Xiong
APAC Risk Transformation Leader
steven.xiong@ch.ey.com
+86 21 2228 2688

OCEANIA

Hanny Hassan
Oceania Financial Services
Organization
Technology Risk Leader
nanny.nassan@au.ey.com
+61 2 9248 4141

Heidi Riddell
APAC and Oceania Risk Leader
heidi.riddell@au.ey.com
+61 2 9248 4569

EUROPE, MIDDLE EAST, INDIA AND AFRICA (EMEIA)

Kanika Seth
EMEIA Financial Services
TPRM Leader
kseth@uk.ey.com
+44 20 7951 7469

Netta Nyholm
EMEIA Risk Management Leader
netta.nyholm@de.ey.com
+49 221 2779 16427