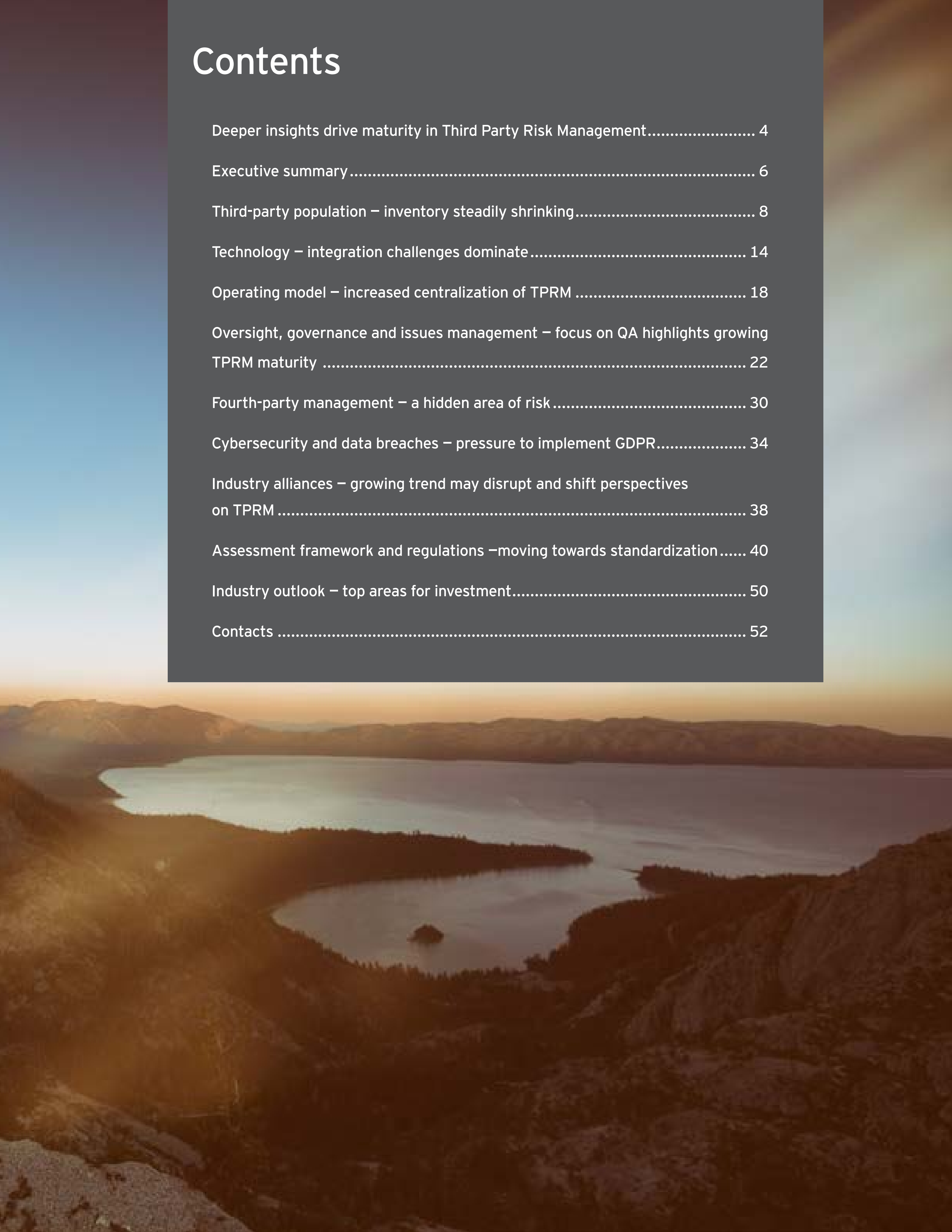
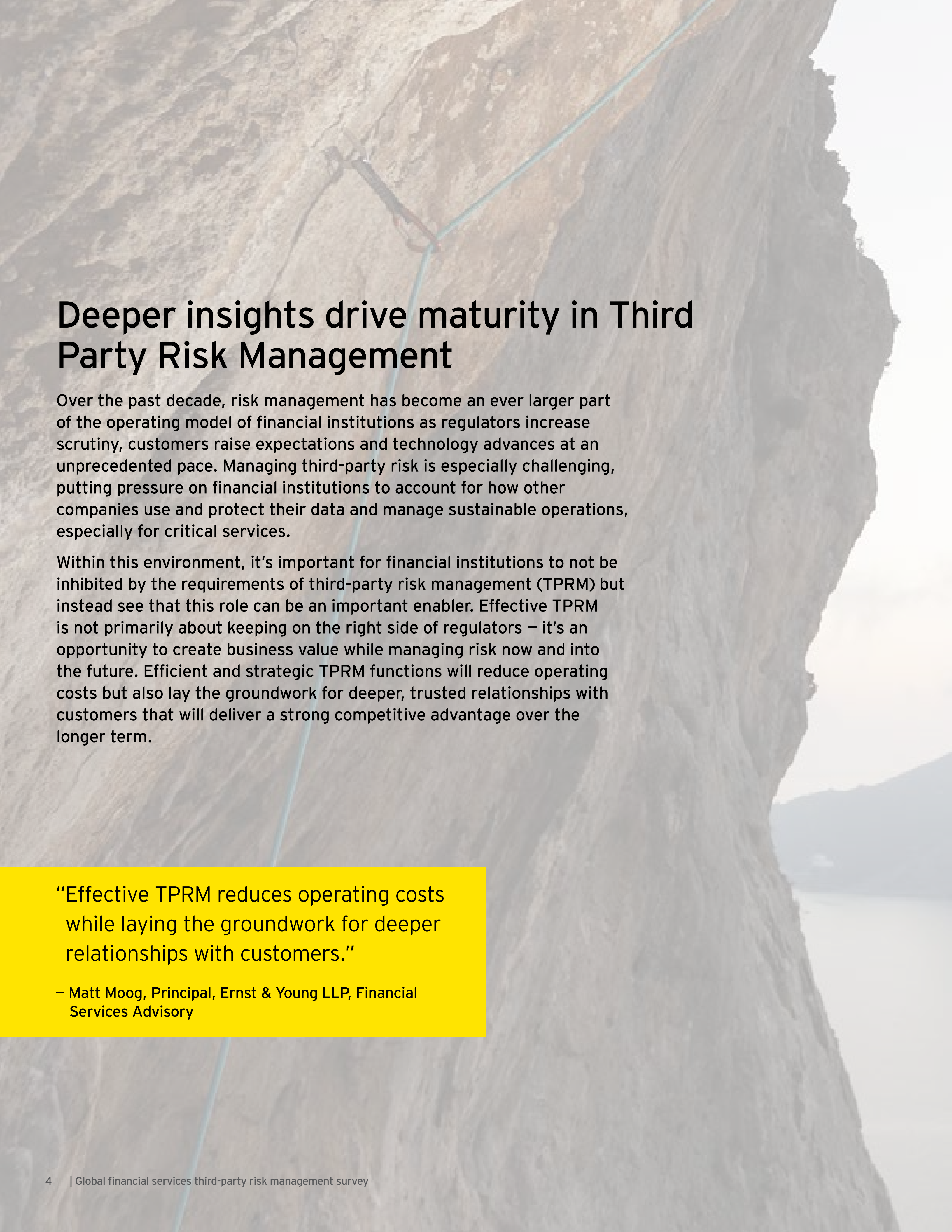
Global financial services third-party risk management survey

Is it time to shift your perspective of third-party risk?

Building a better working world



Contents

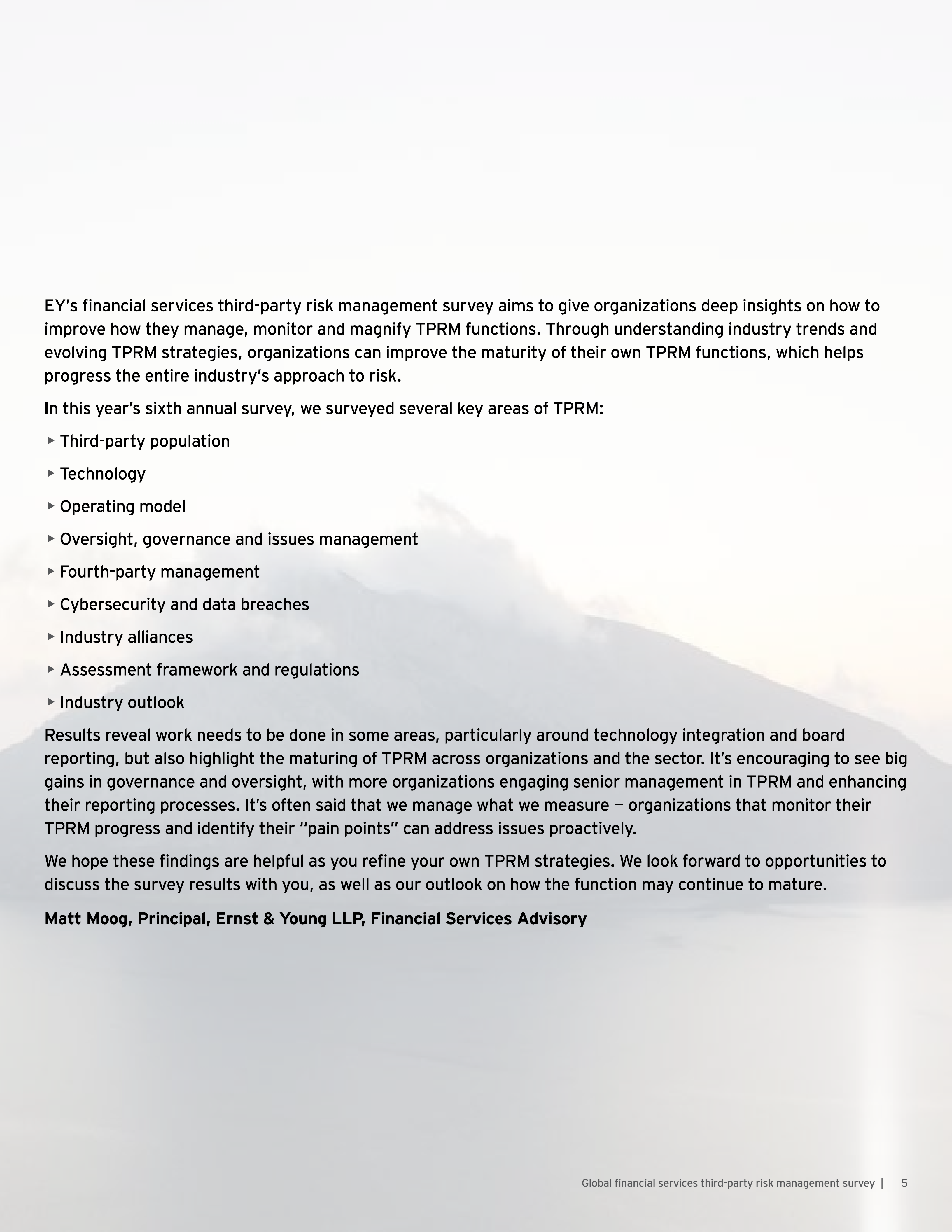


Deeper insights drive maturity in Third Party Risk Management

Over the past decade, risk management has become an ever larger part of the operating model of financial institutions as regulators increase scrutiny, customers raise expectations and technology advances at an unprecedented pace. Managing third-party risk is especially challenging, putting pressure on financial institutions to account for how other companies use and protect their data and manage sustainable operations, especially for critical services.

Within this environment, it's important for financial institutions to not be inhibited by the requirements of third-party risk management (TPRM) but instead see that this role can be an important enabler. Effective TPRM is not primarily about keeping on the right side of regulators — it's an opportunity to create business value while managing risk now and into the future. Efficient and strategic TPRM functions will reduce operating costs but also lay the groundwork for deeper, trusted relationships with customers that will deliver a strong competitive advantage over the longer term.

> "Effective TPRM reduces operating costs while laying the groundwork for deeper relationships with customers."
>
> — Matt Moog, Principal, Ernst & Young LLP, Financial Services Advisory



EY's financial services third-party risk management survey aims to give organizations deep insights on how to improve how they manage, monitor and magnify TPRM functions. Through understanding industry trends and evolving TPRM strategies, organizations can improve the maturity of their own TPRM functions, which helps progress the entire industry's approach to risk.

In this year's sixth annual survey, we surveyed several key areas of TPRM:

- Third-party population
- Technology
- Operating model
- Oversight, governance and issues management
- Fourth-party management
- Cybersecurity and data breaches
- Industry alliances
- Assessment framework and regulations
- Industry outlook

Results reveal work needs to be done in some areas, particularly around technology integration and board reporting, but also highlight the maturing of TPRM across organizations and the sector. It's encouraging to see big gains in governance and oversight, with more organizations engaging senior management in TPRM and enhancing their reporting processes. It's often said that we manage what we measure — organizations that monitor their TPRM progress and identify their "pain points" can address issues proactively.

We hope these findings are helpful as you refine your own TPRM strategies. We look forward to opportunities to discuss the survey results with you, as well as our outlook on how the function may continue to mature.

Matt Moog, Principal, Ernst & Young LLP, Financial Services Advisory

Executive summary

Our latest survey of third-party risk management (TPRM) within financial services organizations shows that most have made significant upgrades and enhancements to the governance and oversight of this critical function. Challenges continue to persist in various areas, including integration of technology across the entire end-to-end third-party life cycle and accurate and timely reporting of third-party program metrics.

Overall, there has been an encouraging maturation of third-party programs, primarily due to continued enhancements to regulatory requirements from the Office of the Comptroller of the Currency (OCC) in 2017 and the emphasis of banking organizations in our population response. Many organizations continue to adjust the overall structure and scope of their risk management programs, emphasizing centralization of functions, rationalization of the third-party population (both overall and in scope for risk management) and rightsizing of quality assurance (QA) and quality control (QC) functions. As banks are subject to a higher level of regulatory scrutiny, these firms' third-party risk management programs tend to be well established and more mature and robust than those within insurance providers and asset managers.

Survey highlights

Third-party population

- Over two-thirds (68%) of organizations report that less than a quarter of their total third population is in scope for the TPRM program, up from 47% three years ago. This indicates improvements in organization's showing ability to scope, assess and prioritize risks.

Technology

- Nearly all organizations (96%) have not reached the optimized level of technology integration, while 81% are neutral or negative in terms of how well their technology integrates and captures risk for reporting.

Operating model

- Centralization of the TPRM function continues to increase, with 57% of organizations having a centralized structure, compared to 45% in 2016. Only 7% of organizations still use a decentralized model, down from 14% in 2016.

Oversight, governance and issues management

- Third parties with breaches or incidents are reported to the board at less than a quarter of organizations; however, senior management is involved in more than 60% of organizations.

Fourth-party management

- Over half (60%) of organizations that identify fourth parties do not maintain an inventory for monitoring and governance purposes.

Cybersecurity and data breaches

- All organizations responded that it will take at least a moderate effort to implement General Data Protection Regulation (GDPR) requirements.

Industry alliances

- Around half (44%) of organizations have considered using an alliance or consortium to obtain efficiencies in certain areas, including for a common assessment framework, assessment service provider or common assessment resources.

Assessment framework and regulations

- Nearly three-quarters (72%) of organizations are using industry-standard questionnaires or have built their questionnaires by using a standard as a baseline, up from 44% in 2016. Fewer organizations (28%, down from 46% in 2016) are using completely proprietary questionnaires for third-party assessments.

Future outlook

The significant challenges cited across the industry around technology integration for the entire third-party life cycle are reflected in many respondents reporting an increased focus on further investment in this area. Ninety-four percent of organizations also plan to spend more or the same on third-party risk technology enablement in 2018 with the aim of improved governance and reporting. Most organizations also plan to use assessment and information sharing through alliances or industry utilities to better address some of the due diligence and ongoing monitoring requirements of a third-party risk management program.

> "The main focus is on the use of technology as a workflow tool, a reporting mechanism and as a way to enhance the risk management of our third-party relationships."
>
> – Financial services executive

> "This year's survey yielded the most responses to date. Results show that in areas such as risk models, assessment approaches and governance, firms have reached common ground. However, not surprisingly, technology and regulations such as GDPR continue to be a significant challenge."
>
> – Chris Ritterbush, Executive Director, Ernst & Young LLP

Third-party population — inventory steadily shrinking

At a glance

- Over two-thirds (68%) of organizations report that only 1 in 4 third parties are in scope for the TPRM program, significantly up from the 47% of organizations that reported three years ago. It was also found that only 6% of organizations had all third parties in scope, down from 19% three years ago, showing an easing from intense regulatory scrutiny on the concept of "all" third parties being in scope.
- Organizations continue to include fewer third parties in the two highest risk tiers, enhancing the focus of due diligence on the highest-risk third parties. This year, almost 75% of organizations reported that fewer than 10% of their third parties were in their highest risk tier, up from 50% in 2016.
- The majority of organizations reported that critical third parties are defined using potential to impact critical business processes and the sensitivity of data involved in processing the service organization, as defined by the Consumer Financial Protection Bureau (CFPB).

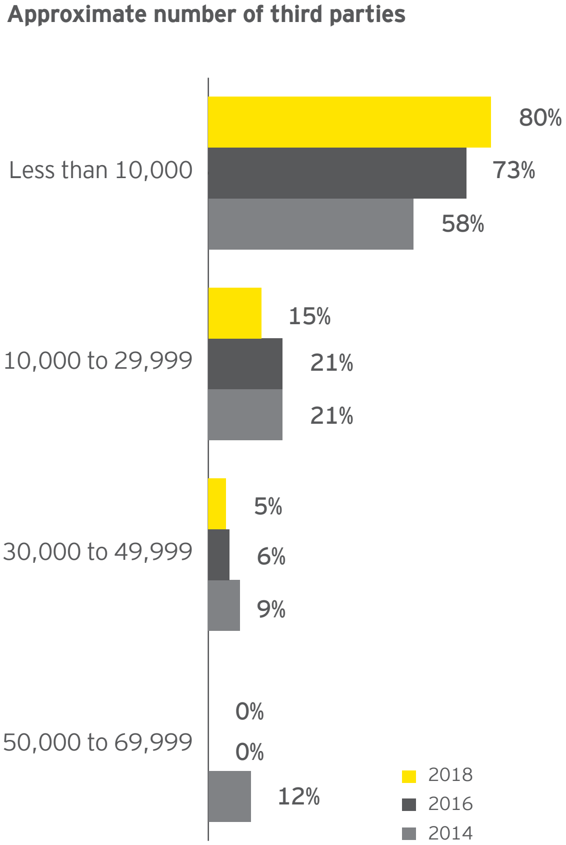
Decreased scope allows sharper focus on higher-risk third parties

The size of organizations' third-party inventory has decreased steadily for the past four years. Now, 80% of organizations surveyed have fewer than 10,000 third parties in their inventory, versus 58% three years ago.

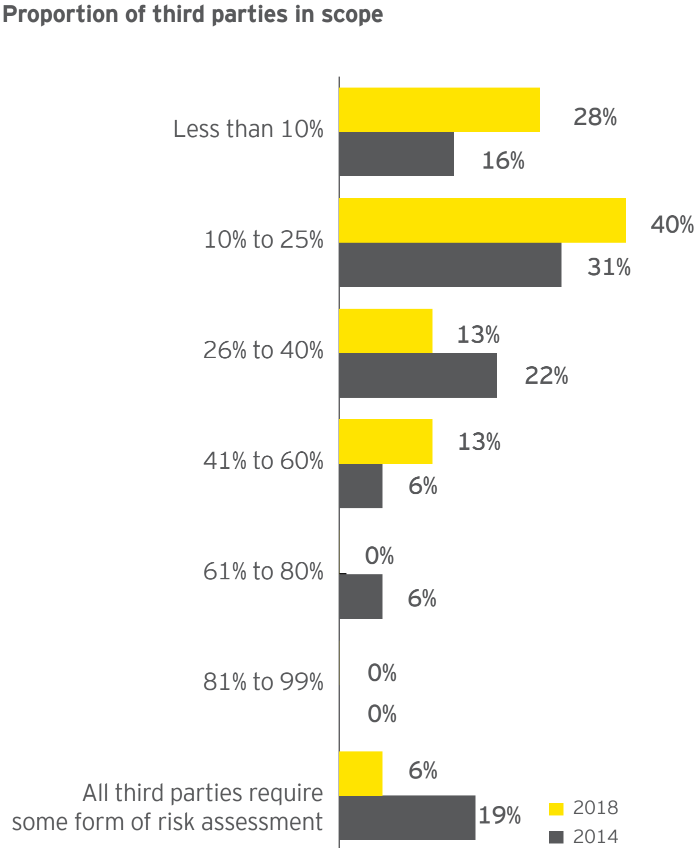
Organizations continue to reduce the number of third parties in their inventories, though it is worth noting that there was a slight decrease in the average amount of employees at organizations who responded to the survey. While this may partially account for the overall decrease in number of third parties, this also highlights that smaller organizations are continuing to be more involved in third-party risk management across the industry. Six additional organizations with fewer than 25,000 employees responded to this year's survey, while the number of organizations with over 25,000 employees was essentially unchanged.

Organizations continue to enhance their methodologies to better scope, assess and prioritize risks of third parties. This steep decrease in scope enables organizations to focus their resources and efforts on higher-risk third parties and reduce costs of lower-value efforts.

Third-party inventory
Approximately how many third parties are within your organization's inventory/population?



Proportion of third parties in scope for risk
What percentage of third parties are in scope for your organization's risk management program?

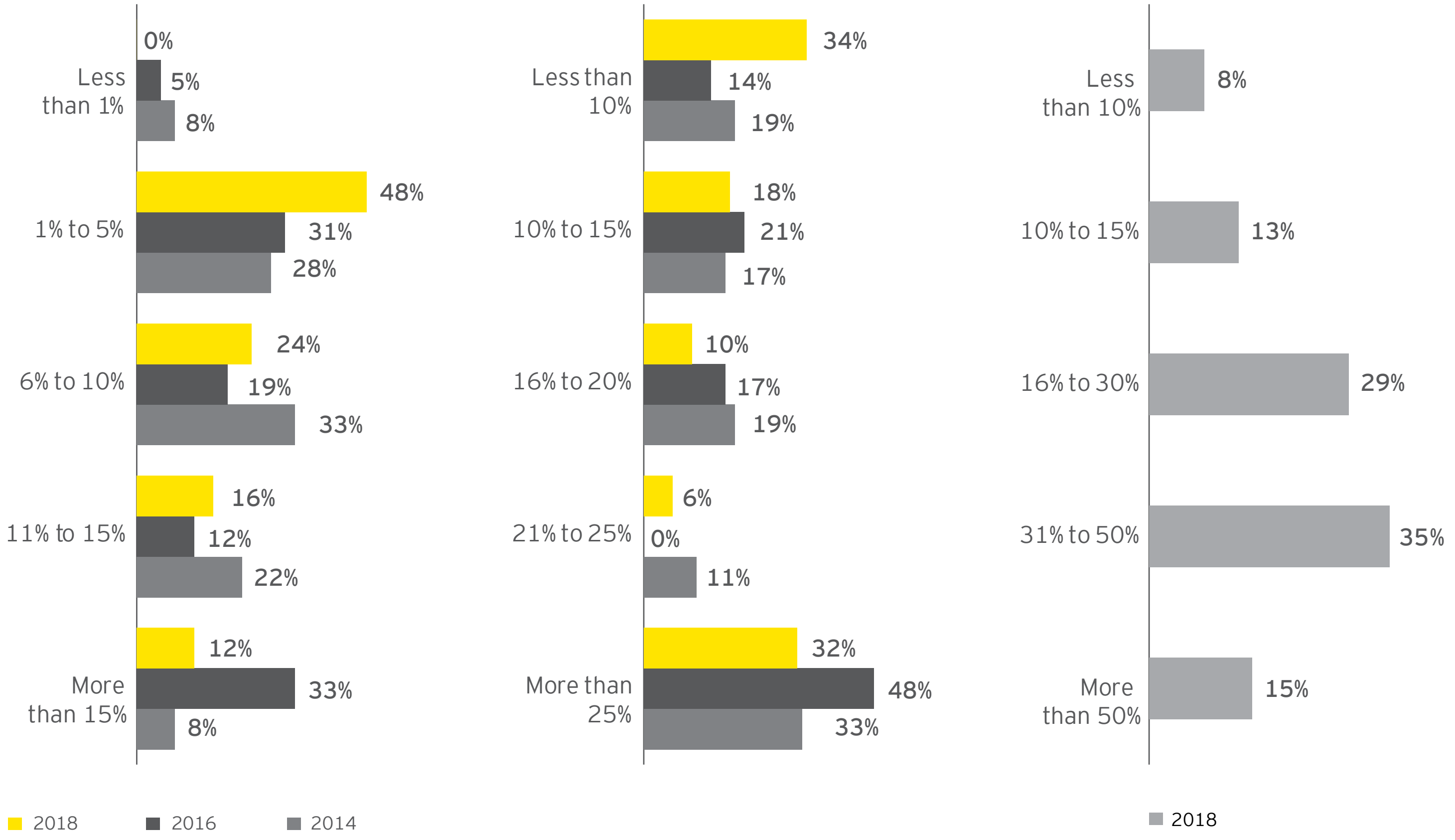


Fewer third parties in highest risk tiers

Organizations continue to include fewer third parties in the two highest-risk tiers, enhancing the focus of due diligence on the highest-risk third parties. This year, almost 75% of organizations reported that fewer than 10% of their third parties were in their highest risk tier, up from 50%, while 62% of organizations noted that fewer than 20% of their third parties were in the second highest risk tier. The third highest risk tier contains the highest proportion of third parties, with 79% of organizations reporting 15% or more of their third parties are in scope for monitoring and assessment.

These results, in conjunction with the majority of organization only including a quarter of third parties in scope for risk assessment, indicates that organizations are making progress in segmenting risk associated with third parties. This enables organizations to hone in on higher risk third parties more effectively and make better risk decisions.

Most organizations reporting fewer than 10% of their third parties in their highest risk tier also signifies that the market has finally absorbed the impact of the mortgage crisis and rightsized high-risk portions of their program back to reasonable pre-crisis levels.



Proportion of third parties in highest risk tier

Proportion of third parties in second highest risk tier

Proportion of third parties in third highest risk tier

More organizations identify critical third parties

The majority of organizations reported that critical third parties are defined using potential to impact critical business processes and the sensitivity of data involved in processing the service.

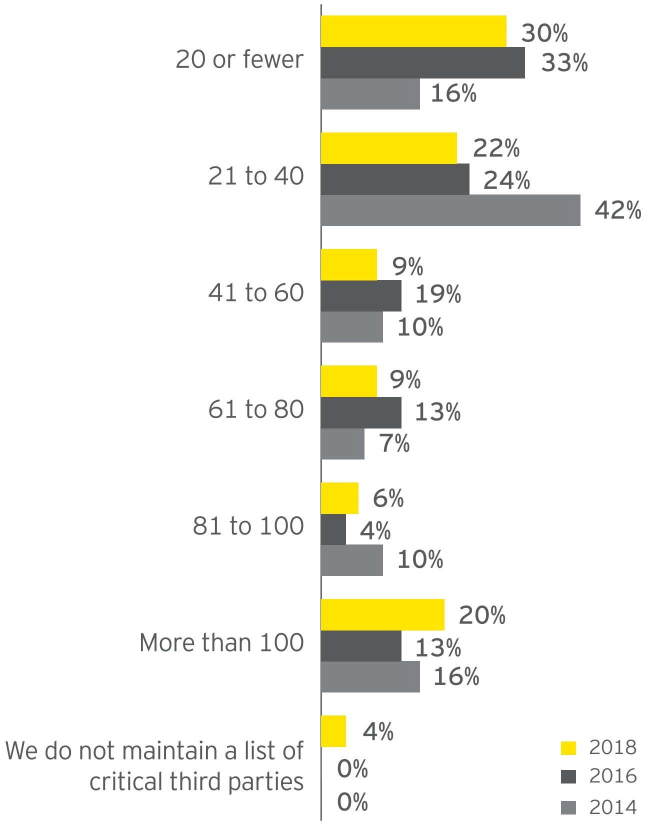
Over 95% of organizations surveyed maintain a list of critical third parties, up from 90% in 2016. Of the firms that maintain a critical listing, approximately 50% keep the list to no more than 40 third parties and three-quarters have fewer than 80 on their listing.

However, the percentage of organizations that maintain a list beyond 100 critical suppliers has increased to 20% from 13% two years ago.

Critical third-party listings enable the board to focus on the critical failure points and will demand an additional level of evaluation, reporting and oversight. In many cases, reporting is required directly to the local country regulator for changes to these populations, and we have seen a number of MRAs (matters requiring attention) within the banking community focused on the differentiation of critical third-party oversight from the other risk tiers. This will only become more of a focus as regulators grasp the concept of industry- and sector-critical third parties seen in recently proposed guidance.

Number of critical third parties

How many critical third parties are within the organization's third-party inventory?



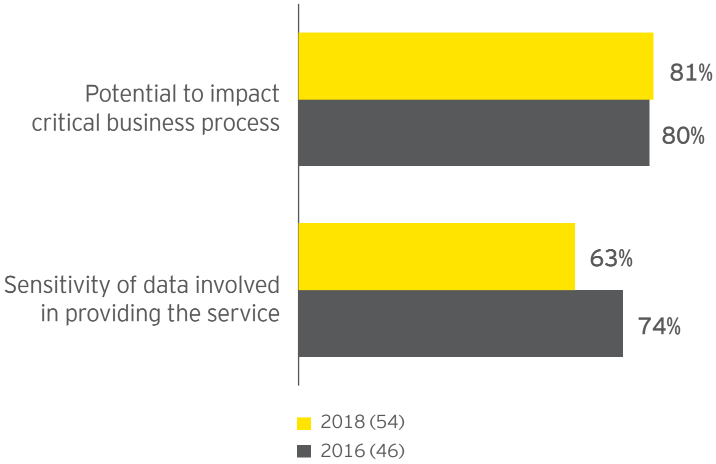
Agreement on definition of critical third parties

The majority of organizations continue to agree that the following criteria should be used to determine a critical third party:

- Potential to impact critical business processes (81%)
- Sensitivity of data involved in providing the service (63%)

It should also be noted that the primary criteria for defining critical third parties includes important drivers for evaluating the risk for all third parties.

Defining critical third parties - most important criteria



Technology — integration challenges dominate

At a glance

- A considerable percentage of organizations (43%) feel negative about how well their TPRM tools integrate and capture the overall risk for reporting purposes, while an additional 38% feel neutral. Over 40% of organizations feel that there is significant room to integrate further. Less than 20% feel positive about their technology integration and ability to capture risk for reporting.
- Despite continued technology investments over the past several years, 89% of third-party inventories require manual updates when a new service is added.

Lack of integration exposes gaps in risk reporting

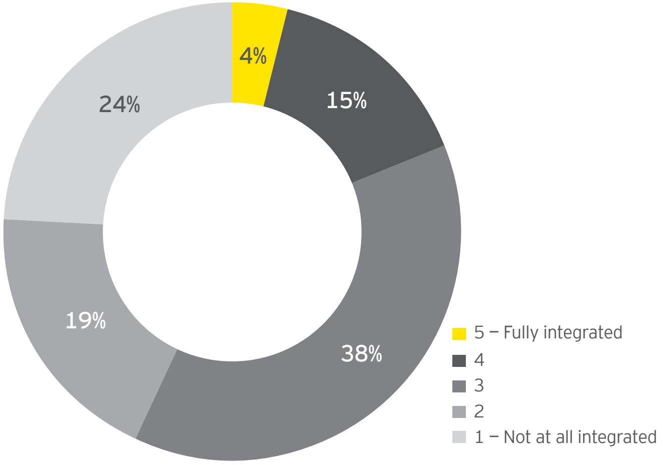
As investments in TPRM technology platforms continue to rise, integration with other tools has not kept pace.

Fewer than 20% of organizations surveyed feel that their technology environment is either fully or largely integrated. In fact, just over 40% feel that there is significant room to integrate further. These figures support the consistent lack of progress organizations are making with regards to successful technology integration for overall risk reporting purposes. As a collective group, less than 1 in 20 organizations would refer to their technology as fully integrated.

> “We’ve got disparate systems. We need to get those systems more integrated. You know, there’s a lot of information out there that’s available regarding risk and probably regarding operational performance as well. There’s a lot of information available, and it’s really where technology could assist in gathering that information.”
>
> — Asset management executive

On a scale of 1–5, with 1 — not at all integrated and 5 — fully integrated, how well do your TPRM tools integrate and capture the overall risk for reporting purposes?

Technology integration



Most firms yet to automate inventory updates

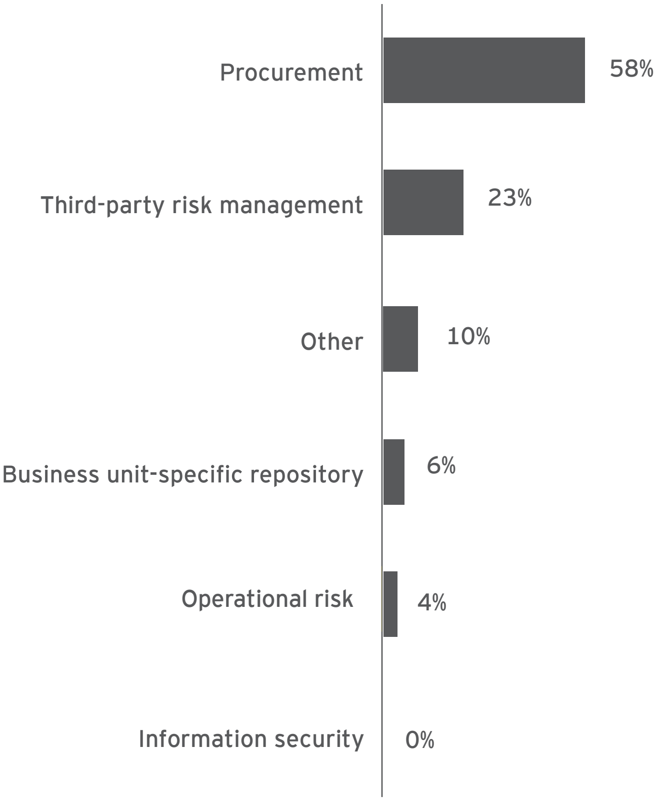
Procurement is the most common owner of the “golden source” of the third-party inventory across more than half of the organizations.

While technology platforms continue to be leveraged to obtain operational efficiency, 89% of organizations still rely on some type of manual update when updating their third-party inventories with new services.

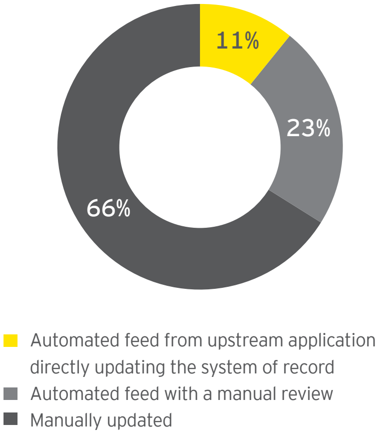
Just one in three firms has an automated process to update the golden source inventory, and even two out of three of those firms require a manual review to confirm the update was accurate and complete.

What functional department owns the golden source third-party inventory?
How is the golden source third-party inventory updated with net new services?

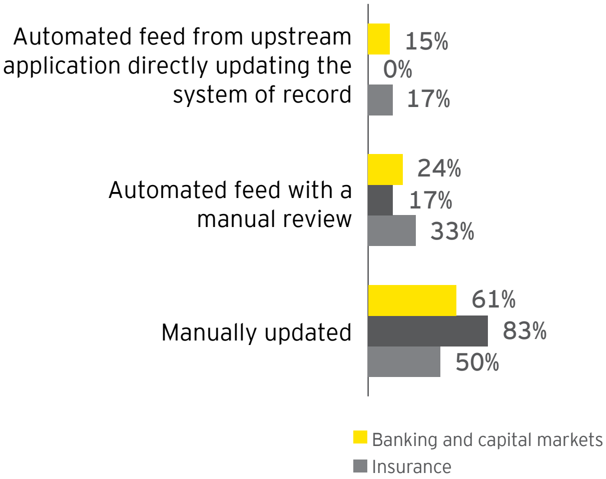
Department in charge of "golden source" record of third-party inventory



Third-party inventory update method



Third-party inventory update method



GRC enabling technology usage continues to rise

Since 2016 we have seen that an increased number of organizations use their governance, risk and compliance (GRC) tool for TPRM functions. Currently over 70% of organizations surveyed use GRC tools for inherent risk assessments, control assessments and issue management, while 50% of organizations entrust the storage of their third-party inventory to the same system.

In 2016 there was no real consensus across the industry around which specific technology was preferred, but Archer was leading the GRC pack with 33% of respondents using its technology. In 2018 that trend continued, with Archer picking up roughly 10% gains, when being leveraged for inherent risk assessment, issue management control and control assessment facilitation.

	Archer	
	2016	2018
Sourcing activity	7%	9%
Inherent risk assessment	26%	34%
Contract repository	4%	4%
Primary third-party inventory	26%	24%
Control assessment facilitation tool	30%	41%
Issue management tool	26%	34%

Operating model — increased centralization of TPRM

At a glance

- Over a third (37%) of organizations said that primary ownership of third-party risk management resides within the procurement function, slightly up from 35% in 2016. It is worth noting that there is still no clear consensus as to who owns the program. Across the industry information security (6%), operational risk (17%), enterprise risk (13%) and business lines (19%), each owns the program at a meaningful number of firms.
- Centralization of the TPRM function continues to increase, with 57% of organizations having a centralized structure, compared to 45% in 2016. Only 7% of organizations still use a decentralized model, down from 14% in 2016.
- There is very little consistency in the responsibility and ownership of different functional components of TPRM, showing that organizations are unique in deploying ownership structures and operating models that reflect the structure and culture of their own organizations.

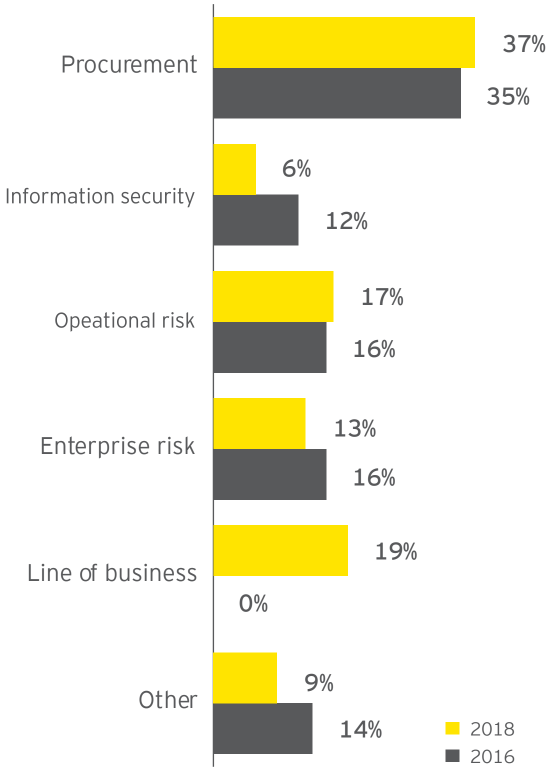
Procurement is most likely home for TPRM

Over a third (37%) of organizations said that primary ownership of third-party risk management resides within the procurement function, up slightly from 35% in 2016. It is worth noting that there is still no clear consensus as to who owns the program. Across the industry, information security, operational risk, enterprise risk and business lines owns the program at a meaningful number of firms.

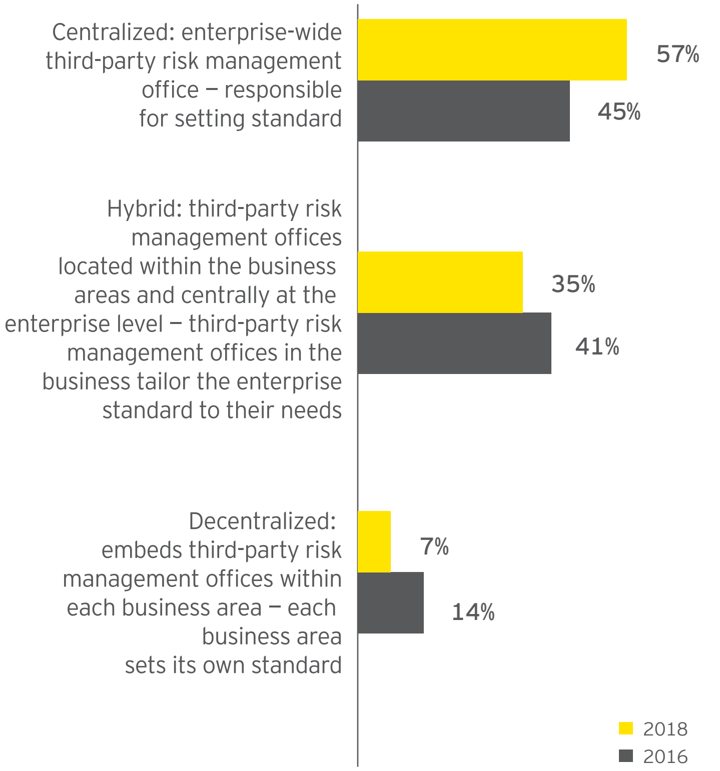
Centralization of the TPRM function continues to increase, with 57% of organizations having a centralized structure, compared to 45% in 2016. Only 7% of organizations still use a decentralized model, down from 14% in 2016. It was also found that there is very little consistency in the ownership of different functional components of TPRM, driving the need for increased centralization in the future. This significant trend shows that organizations continue to move away from each business area having embedded risk management functions to handle key TPRM activities and a push toward one focused TPRM function, responsible for setting the standard for all business areas.

Primary ownership and structure of TPRM function
What area has primary ownership of the third-party risk management function?
How is your third-party risk management program structured?

Primary ownership of TPRM program



Structure of TPRM



Organizations align TPRM activities across numerous parts of the business

There is currently very little consistency in the responsibility and ownership of different functional components of TPRM, showing that organizations are unique in deploying ownership structures and operating models that reflect the structure and culture of their own organizations. However, we are seeing a consistent shift towards centralizing ownership of the TPRM function with responsibility for setting program expectations, structure, strategy and direction.

While firms have begun to centralize the main TPRM resource group, there is still little consensus for where most of these functions are executed. Organizations have been successful at centralizing in certain areas of the function, and unsuccessful in others. Organizations have successfully centralized primary responsibility for performance monitoring (87%) and exit strategy (74%) within the lines of business. Procurement is also typically responsible for notification of upcoming and expired contracts (66%) and termination of contracts (57%).

There have also been areas in which there is no consensus as to which is the responsible party, including SOCR (Service Organization Control s Reporting) report reviews, business continuity assessments and local country risk assessments.

> “We’re continually making enhancements to the program to strengthen it. I’d say that the two biggest are an effort to centralize some aspects of the execution around third-party risk management and the direction to club together with some other banks to form a joint venture to help us with some of the data collection and assessment work.”
>
> **— Global banking executive**

Primary responsibility for TPRM functions
Which functional area has primary responsibility for the execution of the following components of your organization's third party risk management program?

Third-party risk management responsibility

	Procurement	Information security	TPRM	Legal/ general counsel	Operational risk	Compliance	LOB	Other	Not Conducted
Design and administration of the inherent risk assessment	26%	2%	**43%**	0%	20%	0%	4%	6%	0%
Completion of inherent risk assessment	13%	2%	17%	0%	6%	0%	**59%**	4%	0%
Business reputation and qualification review	**35%**	0%	19%	0%	9%	4%	28%	4%	2%
Anti-corruption/ anti-bribery review	9%	0%	9%	4%	7%	**44%**	**4%**	13%	9%
Anti-money laundering (AML)/ economic sanction review	13%	0%	9%	4%	9%	**45%**	4%	13%	2%
Performance monitoring	6%	0%	4%	2%	0%	0%	**87%**	2%	0%
Exit strategy	7%	0%	7%	6%	0%	0%	**74%**	2%	4%
Financial viability assessment	**40%**	0%	15%	2%	6%	0%	15%	23%	0%
Country risk assessment	13%	4%	19%	2%	9%	2%	15%	11%	25%
Information security assessment	2%	**85%**	9%	0%	2%	0%	0%	2%	0%
Business continuity assessment	2%	24%	9%	0%	15%	2%	22%	24%	2%
Service organization controls (SOC) report review	4%	26%	15%	2%	6%	0%	33%	7%	7%
Regulatory compliance procedural assessment	2%	2%	7%	2%	9%	**50%**	17%	4%	7%
Regulatory compliance transactional review	0%	0%	6%	2%	6%	**41%**	26%	4%	17%
Issue management/risk treatment	4%	8%	15%	0%	13%	4%	**51%**	4%	2%
Review and update of contract terms as part of ongoing monitoring	37%	2%	0%	22%	2%	0%	30%	4%	4%
Review of issues identified in reviews as part of update to contract terms	24%	4%	4%	11%	6%	0%	**43%**	4%	6%
Identification of expired contracts	**66%**	2%	4%	9%	2%	4%	11%	2%	0%
Notification of upcoming contract expiration	**66%**	4%	6%	11%	0%	2%	9%	2%	0%
Termination of contracts	**57%**	2%	2%	11%	0%	0%	24%	4%	0%

Oversight, governance and issues management — focus on QA highlights growing TPRM maturity

At a glance

- Most (81%) organizations found that reporting on critical third parties was easy and could be done on demand. Reporting on other aspects of the third-party risk management program was generally possible, but may take upwards of a week or more.
- Senior management remains heavily engaged with 60+% of organizations noting that third parties with breaches or incidents, highest levels of inherent risk, significant issues noted and noncompliant third parties are reported to senior management. However, typically less than one-quarter of organizations noted that the same items were reported to the board. Also notable, critical third-party information is only escalated to the board of directors at 41% of organizations, and only 26% of organizations report breaches and incidents to the board.
- The bulk (83%) of organizations have a quality assurance function in 2018, up from 72% having a Quality assurance function last year. As programs mature, we noted an increased focus on quality assurance — peaking at mid-maturity — prior to scaling back the focus at the most mature TPRM programs.
- The majority of organizations (69%+) are incorporating issues and actions plans, inherent risk assessments, control assessments and related evidence into the scope of their quality assurance function. These are the core components of a Quality assurance function, and ultimately, this indicates an increase in the level of maturity and focus of the function since 2016.
- For the first time, more than half of organizations surveyed are using an enterprise-level tool for issue management tracking. This is a big shift from previous years where the issues were primarily managed in spreadsheets. Despite the increased adoption of technology systems, spreadsheets are still a critical component of issue tracking at nearly 40% of organizations.

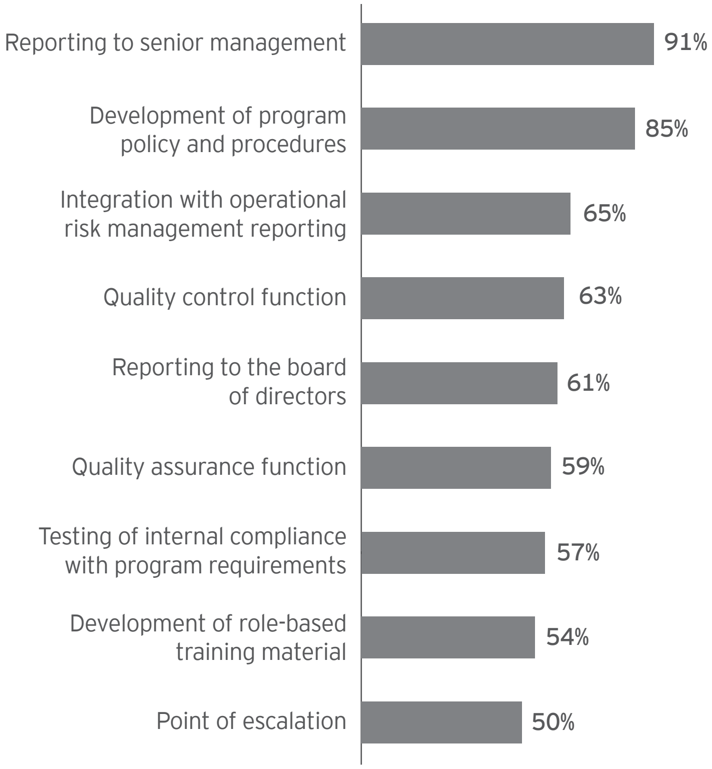
Regulatory scrutiny prioritizes reporting

As regulatory bodies continue to focus on oversight and governance, organizations are also viewing this component of third-party risk management as an area of focus. The vast majority (91%) of organizations surveyed noted that reporting to senior management is a key activity performed as part of oversight and governance, yet when surveyed, less than half of organizations were able to easily report on four out of the six primary TPRM areas.

Reporting to top-level management helps educate the organization on the health of its third-party risk management program, yet less than 27% of reports make it to the board of directors. Although organizations are making progress on their reporting functionality, timely and efficient reporting continues to be a considerable challenge across the industry.

Primary reporting and structure of TPRM function
What activities are performed as part of your organization's oversight and governance program as it related to third-party risk management?

Organizational oversight activities



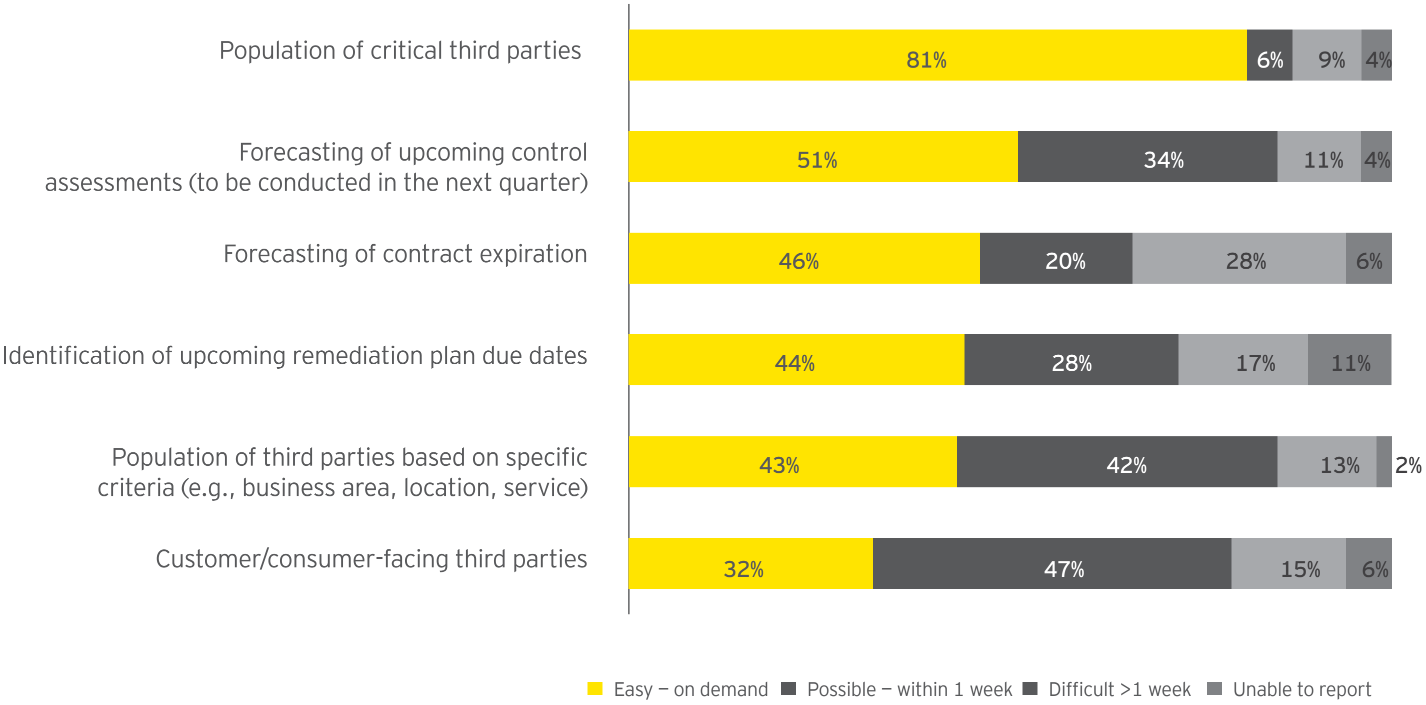
On-demand reporting widespread

Effective third-party risk management reporting provides transparency and accountability and drives valuable conversations with senior management. Four in five organizations (81%) found that reporting on critical third parties could be done on demand; however, reporting on other aspects of the third-party risk management program was generally possible but could take upwards of a week or more.

> "Currently, TPRM-related risks roll up indirectly to risk reporting that goes to the board. Now certainly going forward, a few regulations, such as New York DFS and some other challenges, will probably increase the board visibility and look at third-party risk management program."
>
> — Insurance executive

How quickly would your organization be able to report on the following:

Timeliness of reporting



Critical risks not reported to the board

Senior management remains heavily engaged in risk management reporting, with 60+% of organizations noting third parties with breaches or incidents, highest levels of inherent risk, significant issues noted, and noncompliant third parties are reported to senior management. However, typically less than one-quarter of organizations noted that these items were reported to the board. Also notable, critical third-party information is only escalated to the board of directors at 41% of organizations, and only 26% of organizations report breaches and incidents to the board.

Of the 41% that report on critical third parties to the board, banks lead the way with 53% reporting critical third-party information to the board, while only 25% of insurance firms and 17% of asset managers do. On the flip side, third-party breaches and incidents are only escalated to the board at 21% of banking organizations, 50% of asset managers and 33% of insurance firms.

TPRM reporting hierarchy
When reporting on third-party risk management, what is the level of escalation for each type of report?

Level of escalation for risk management reporting					
	Board of directors	Senior management	Business management	Third-party relationship manager	No reporting
Third parties with breaches or incidents	26%	**70%**	59%	54%	0%
Operational metrics of the program	19%	52%	63%	56%	2%
Critical third parties	**41%**	56%	54%	52%	2%
Third parties with the highest level of inherent risk	22%	61%	65%	52%	4%
Third parties with noted significant issues	19%	**70%**	**72%**	52%	0%
Third parties with control issues that are past due	2%	59%	67%	50%	6%
Third parties with the highest residual risk	22%	48%	57%	39%	13%
Noncompliant third parties	13%	63%	74%	48%	6%
Third parties related to an emerging risk	2%	44%	54%	41%	22%
Third parties about to be terminated	0%	20%	**70%**	50%	13%
All third parties	4%	20%	59%	50%	13%
New third parties	4%	24%	**65%**	50%	17%

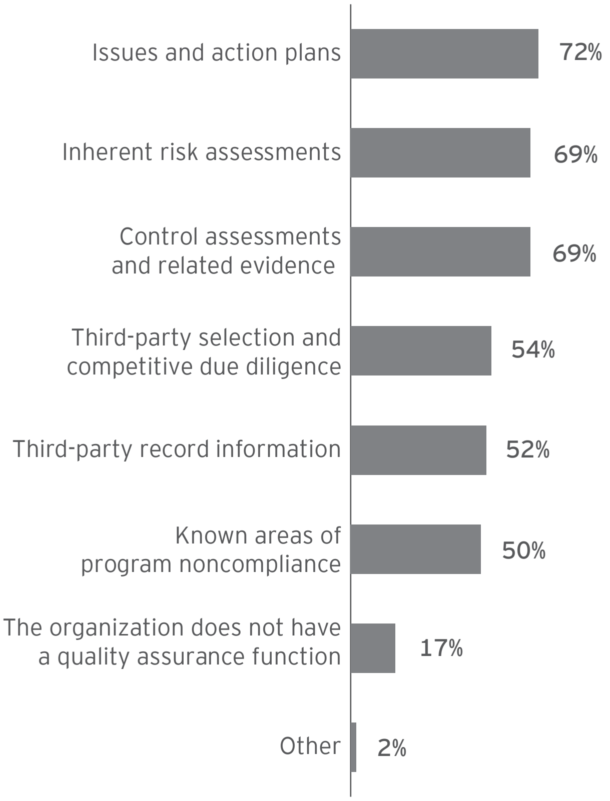
Quality assurance functions indicate maturity

Most organizations (83%) have a quality assurance function in 2018, up from 72% last year. The majority of organizations (69% +) are incorporating issues and actions plans, inherent risk assessments and control assessments, and related evidence into the scope of their quality assurance function. These are core components in scope for the Quality assurance function, and ultimately, this indicates an increase in the level of maturity and focus of the function since 2016.

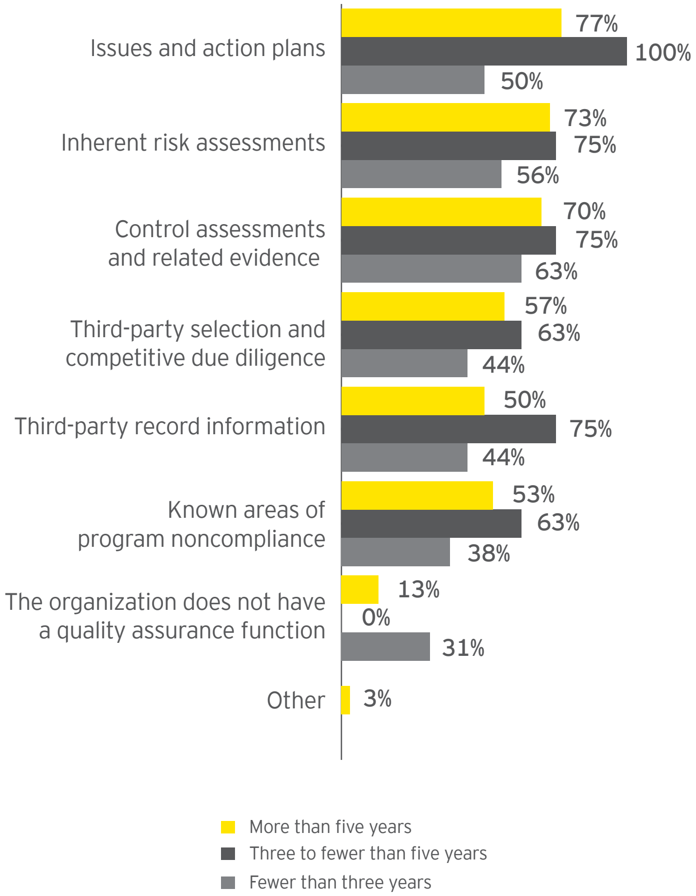
As programs mature, we noted an increased focus on quality assurance — peaking at mid-maturity — prior to scaling back the focus within the most mature programs. Issues and action plans were in scope for the Quality assurance function at 50% of organizations of fewer than three years maturity, compared to being in scope at all organizations with three to five years' maturity, and in scope and 77% of organizations of more than five years' maturity.

What functional components of the program are in scope for the quality assurance function of the third-party management program?

Components in scope for quality assurance of third parties



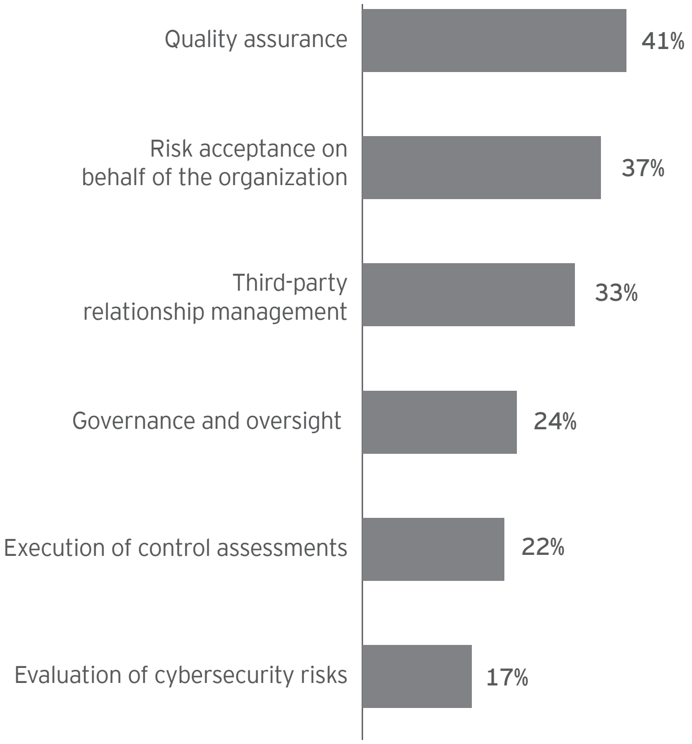
By maturity

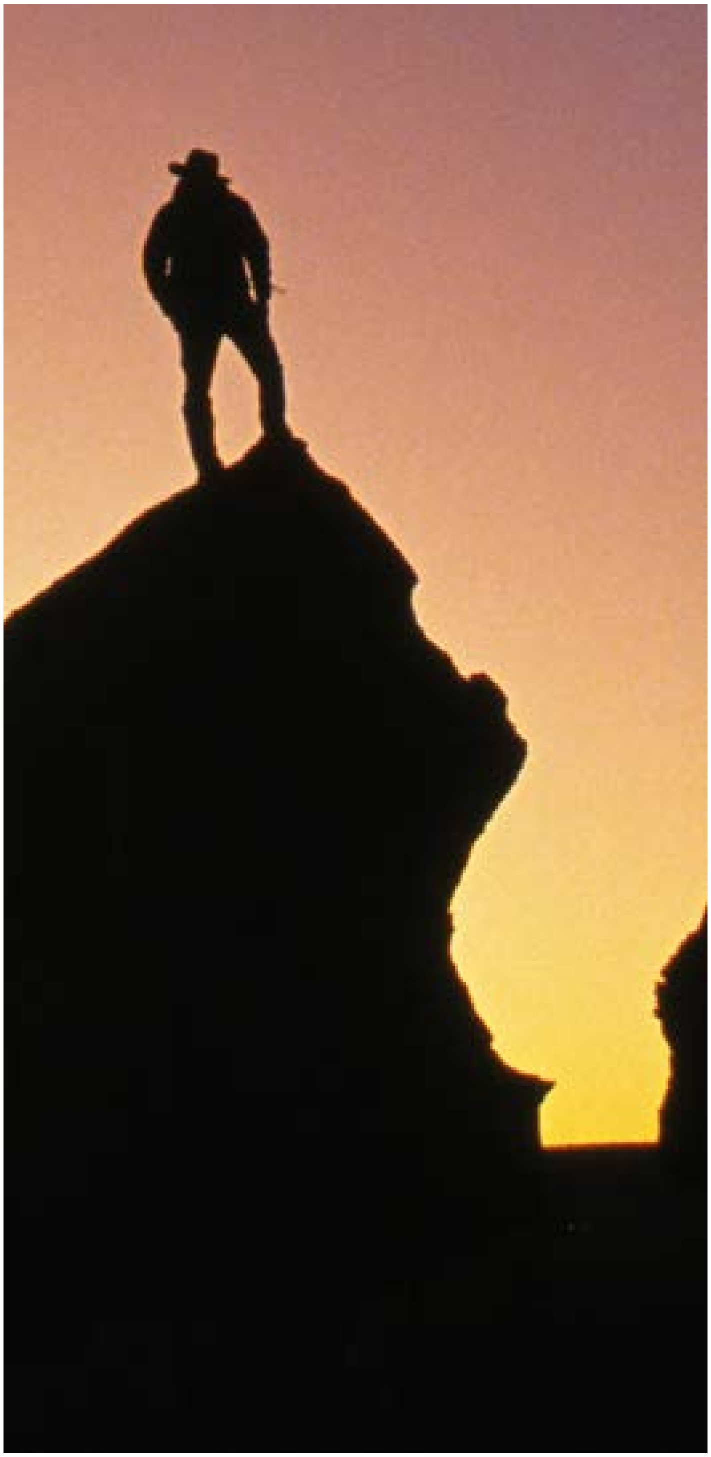


Many organizations reported that there was room to improve the skills of TPRM personnel with the largest percentage focused on an improved Quality assurance function.

Does your organization have the correct skill sets to effectively perform the following activities?

Room to improve the skill sets of individuals performing third-party risk management activities



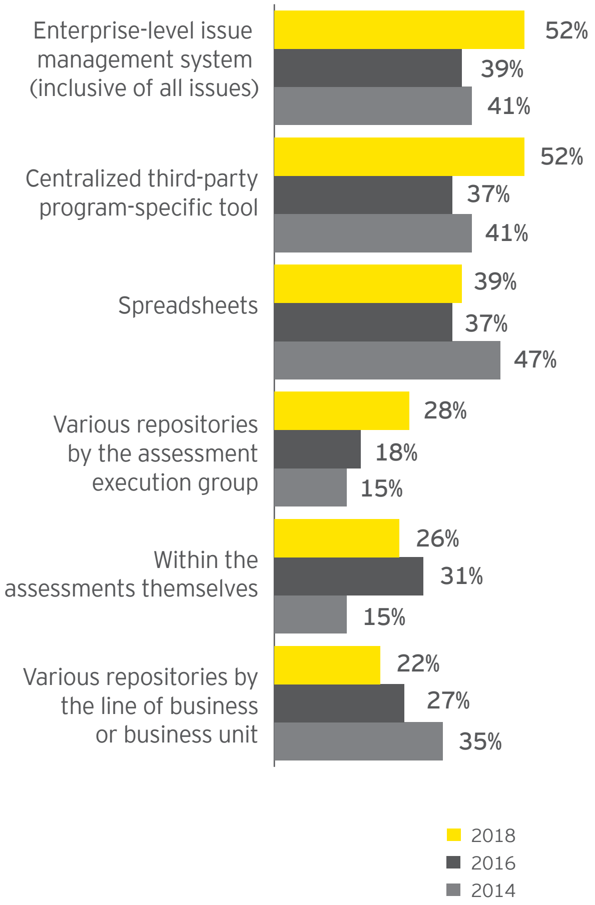


Shift from spreadsheets to enterprise-level tools for issue management

For the first time, more than half of organizations surveyed are using an enterprise-level tool to track issue management. This is a big shift from previous years where the issues were primarily managed in spreadsheets. Despite the increased adoption of technology systems, spreadsheets are still a critical component of issue tracking at nearly 40% of organizations.

How are issues and exceptions stored and tracked?

Storing issues

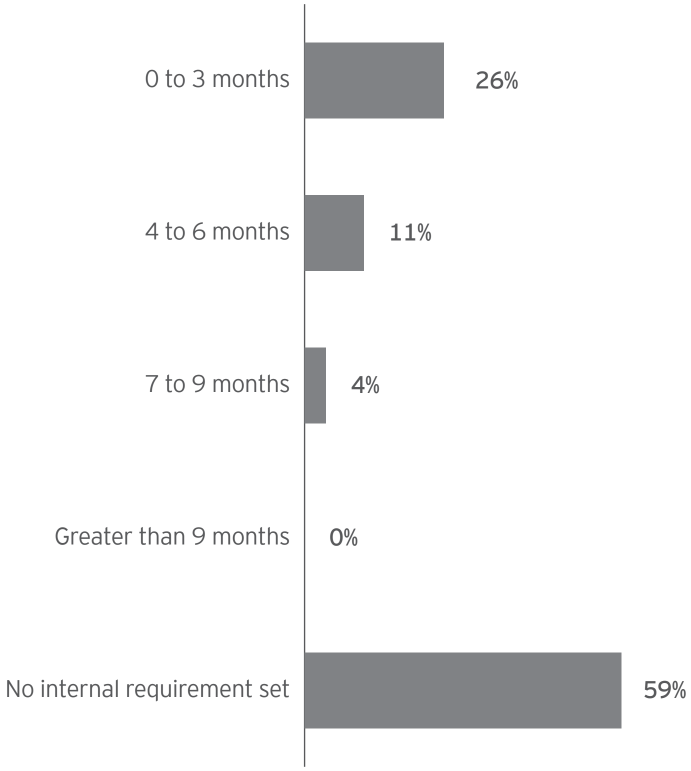


Stricter remediation deadlines could cut risk exposure

Even when remediation plans are developed for high-risk issues, 60% of organizations surveyed do not enforce a strict deadline. When organizations do, it is typically a short window (three months or fewer). This is an area within the industry that can be improved upon to verify that organizations do not have known third-party vulnerabilities open for large periods of time, opening the business up to various risks.

What is your internal requirement for enforcing closure of a remediation plan's close dates for the high-risk issues identified?

Requirement for enforcing closure of remediation plan



> "Firms are eagerly seeking alliances, consortiums and managed services to further improve operational effectiveness and reduce costs. This, along with technology improvement, will be significant efforts in 2018"
>
> **— Chris Ritterbush, Executive Director, Ernst & Young LLP**

Fourth-party management — a hidden area of risk

At a glance

- Six of every 10 organizations that identify fourth parties do not maintain an inventory for monitoring and governance purposes for those parties. Nearly three-quarters (74%) of organizations mentioned that fourth-party concentration risk would be extremely challenging to report on or they could not report on at all.
- Nearly all organizations that identify and/or monitor fourth parties take an indirect approach to performing due diligence. Almost 80% of organizations rely on their third parties for monitoring and assessing their fourth parties.

Tracking fourth parties remains a major challenge

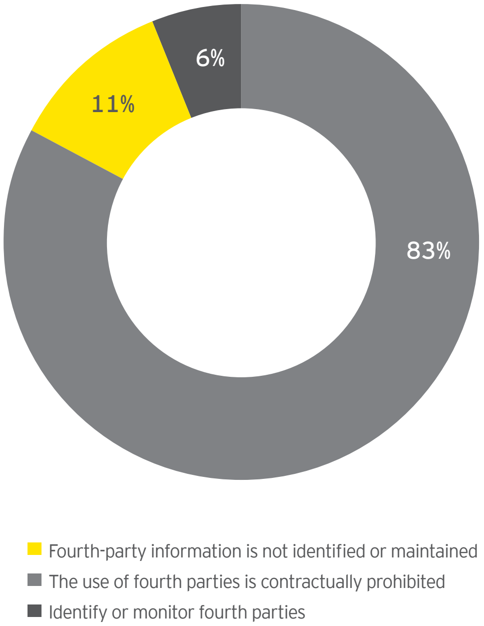
While 83% of organizations reported identifying fourth parties, 60% of organizations that identify fourth parties do not maintain an inventory for monitoring and governance purposes. And 74% of organizations mentioned that fourth-party concentration risk would be extremely challenging to report on, or they could not report on it at all.

Generally, organizations gather information around fourth parties during either the pre-contracting phase or within contracts. However, only 40% of them actually maintain an inventory to track and monitor those fourth parties.

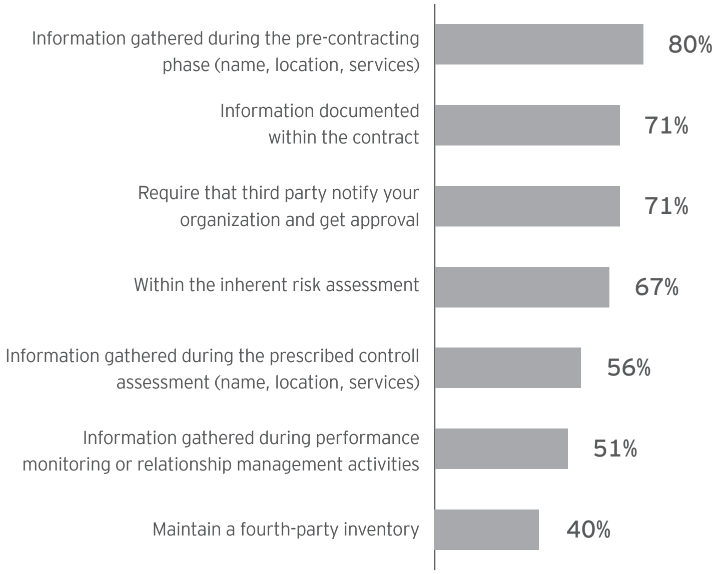
Organizations continue to struggle in understanding their overall risk exposure to fourth parties, heavily relying on their third parties to monitor their activities. The heavy reliance and lack of keen focus on fourth parties create risk to the organizations, including concentration risk of fourth parties, critical failure points at the fourth-party level and data leakage beyond the fourth-party level.

> "I think for us on reporting, one of our challenges is going to be to really evolving our reporting to talk about various concentration risks, and I think there's a couple different ways you can do concentration risk. One focus is around better understanding subcontractors, where they're used, where the same entities are used across multiple of our vendors and the implications of that."
>
> **— Banking executive**

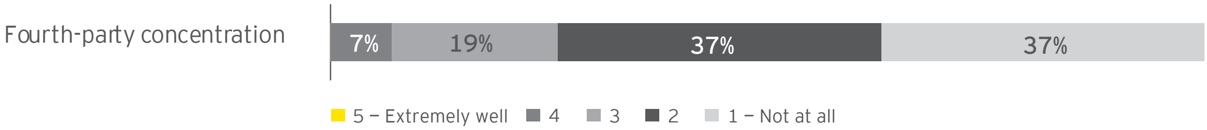
How are fourth parties identified and tracked?



Identify or monitor fourth parties



Ability to report on each type of concentration risk

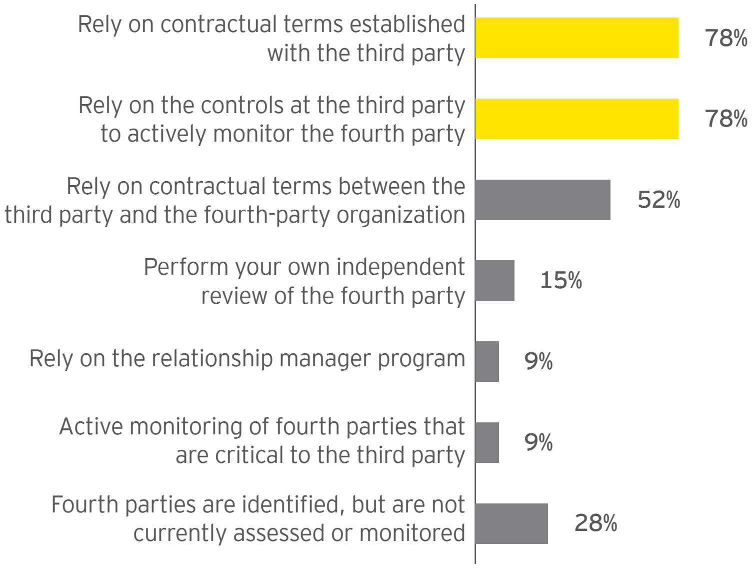


Reliance on third parties for due diligence

Nearly all organizations that identify and/or monitor fourth parties take an indirect approach to performing due diligence. Almost 80% of organizations rely on their third parties to monitor and assess their fourth parties. The two primary approaches for assessing fourth parties are (1) reliance on contractual terms with the third party and (2) reliance on controls at the third party to actively monitor the fourth party. Only 15% of organizations independently review their fourth parties, while 28% of organizations do not assess or monitor fourth parties at all.

How does your organization assess/monitor fourth parties?

Method of assessing/monitoring fourth parties

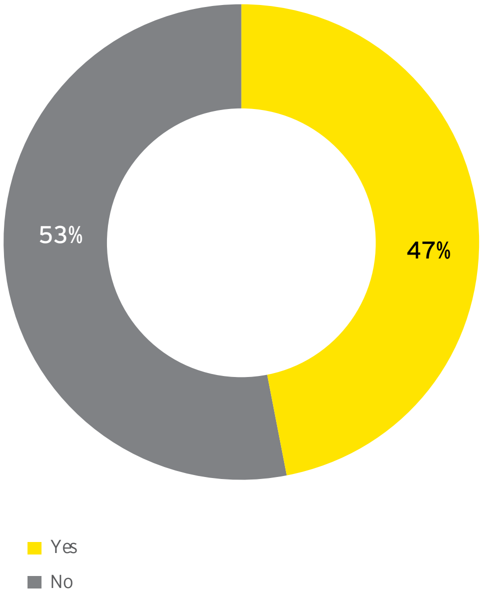


Managing affiliate risk is increasing, especially for banks

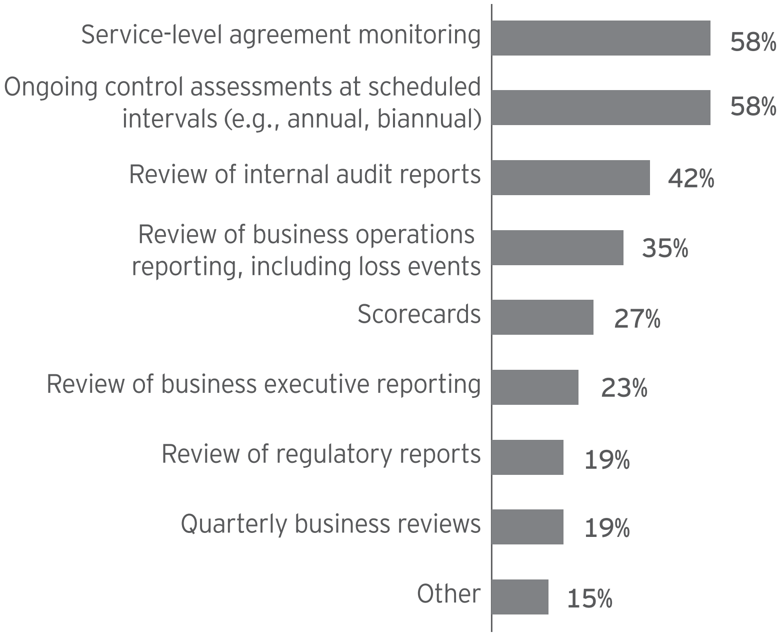
Focus on affiliate management has increased. Nearly half of organizations surveyed have intercompany affiliates that are in scope for their third-party risk management programs. Of the population with intercompany affiliates in scope for third-party risk management, 70% are banks, an industry where the regulatory focus on affiliates is high.

Organizations use a wide variety of techniques to monitor intercompany affiliates. The majority of organizations surveyed have either a service-level agreement in place to monitor affiliates or assess control on a regular basis.

Are intercompany affiliates providing goods/services to your organization's US operating unit in scope for third-party risk management?



Please select all the ongoing monitoring requirements that apply to intercompany affiliates providing goods/services to your organization



Cybersecurity and data breaches — pressure to implement GDPR

At a glance

- All organizations responded that it will take at least a moderate effort to implement General Data Protection Regulation (GDPR) requirements for addressing expectations of informing EU citizens where their personal data is processed and for what purpose if it was outsourced to a third party. Two-thirds of organizations found it significantly challenging to implement the requirements.

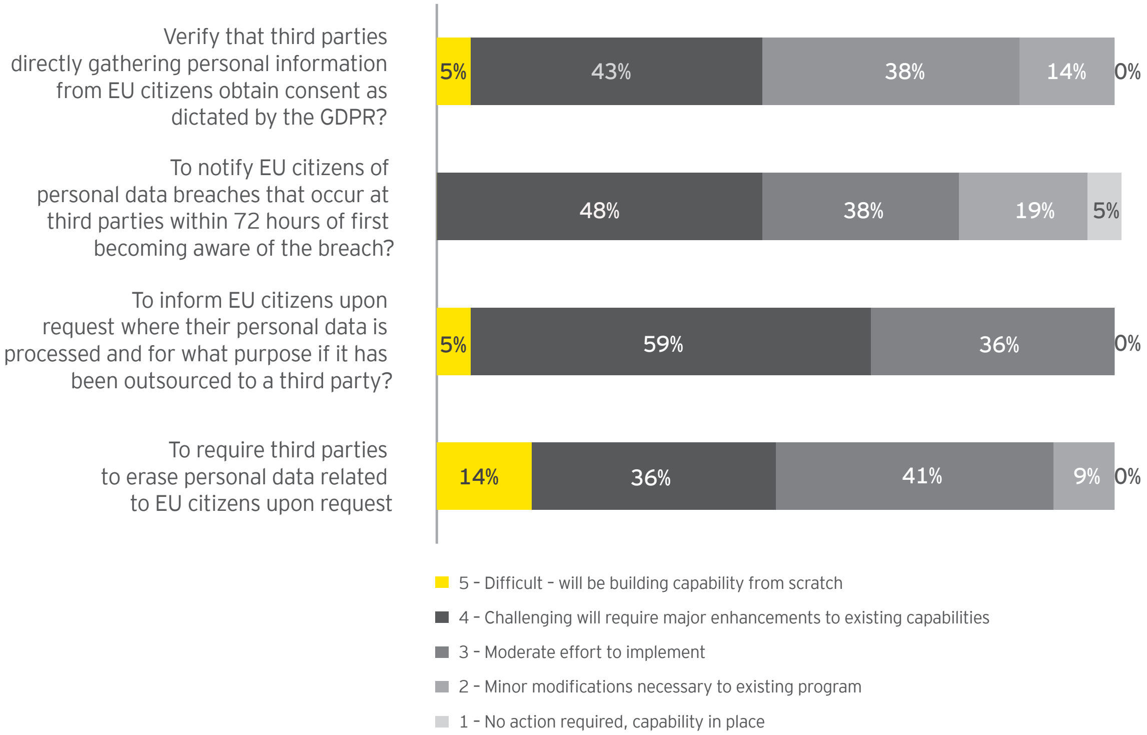
New EU regulations will have global impact

All organizations responded that it will take at least a moderate amount of effort to implement GDPR requirements for addressing expectations of informing EU citizens where their personal data is processed and for what purpose (if it was outsourced to a third party). Two-thirds of organizations found it significantly challenging to implement the requirements. Similar challenges are expected to be encountered complying with other key requirements of GDPR.

Given these challenges, paired with the broader impact of the regulation and the short two-year window for compliance, organizations will need to expend significant energy and effort in the coming year.

Per the EU General Data Protection Regulation (GDPR): On a scale of 1–5, how difficult will it be to address the expectations of the guidance specific to the GDPR as it relates to your third-party population?

Difficulty in addressing GDPR guidance



Cyber ANPR would demand deeper understanding of cyber risks

In October, 2016, the US Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board (FRB) (collectively, the agencies) jointly announced enhanced cyber risk management standards for financial institutions in the form of an advance notice of proposed rulemaking (ANPR). The ANPR outlines enhanced cybersecurity risk management and resilience standards that would apply to large and interconnected entities under the agencies' supervision.

The proposal would apply to third-party service providers with respect to services provided to the covered entities, especially services that support sector-critical systems. Organizations would face considerably higher standards if they desire to continue serving financial institutions that are directly affected, if the proposals are adopted.

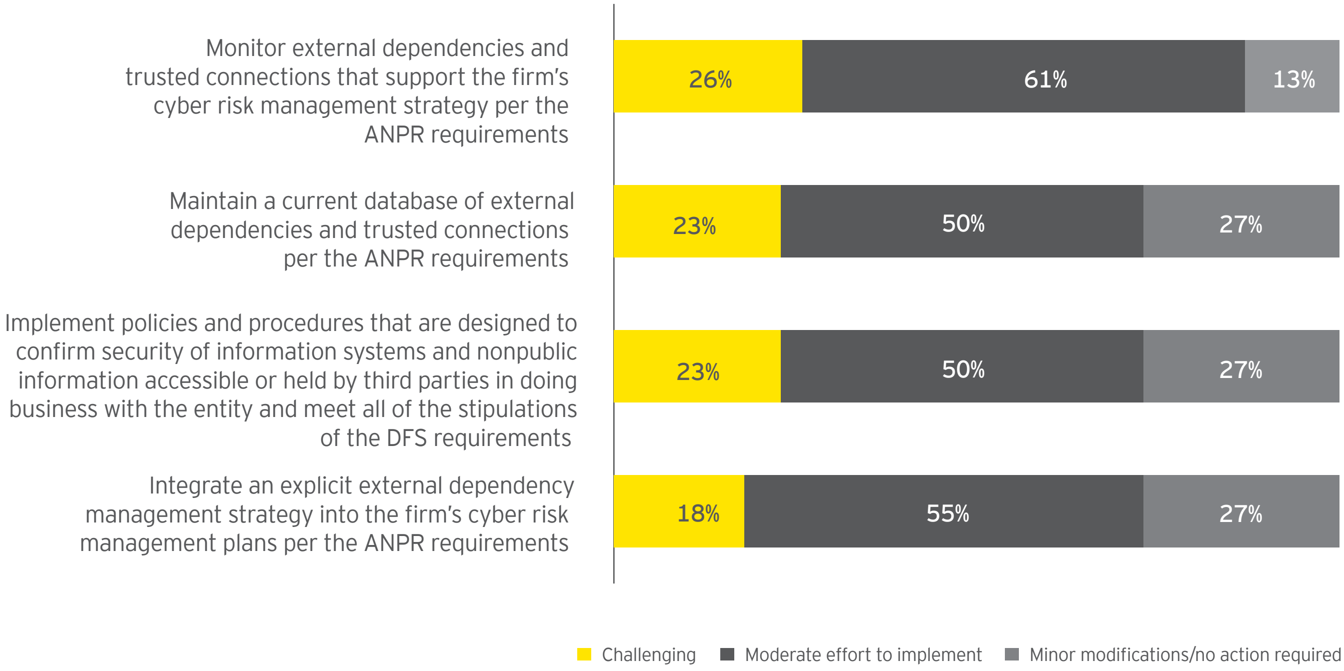
The cyber ANPR set outs a two-tiered set of enhanced standards:

- Standards that apply to all covered entities and covered services provided by third parties
- Higher expectations for those systems deemed critical to the sector (sector-critical systems) and services that support those systems

If the rules were to go into place, organizations would be required to have a much deeper and more comprehensive understanding of the role they play within their ecosystems, their unique cyber risk profile across the ecosystem, and critical dependencies on internal and external parties as a result of the interconnectedness.

Of the organizations we surveyed, we noted, in general, the collective group will have a slightly less difficult time addressing requirements of ANPR than GDPR, with less than a quarter of organizations having significant challenges meeting the four key requirements of the regulation. However, approximately 75% of organizations found it at least moderately difficult to implement the proper controls.

Advanced Notice of Proposed Rulemaking



Opportunity to better align internal reviews with regulatory focus

Oversight and governance and cybersecurity were the most important focus for organizations that have recently had regulatory or internal audit reviews performed on their TPRM programs. In general, there was a large gap in focus between the reviews executed by internal audit and regulatory body — 42% of regulatory bodies deemed oversight and governance as a top area of focus as compared to 70% of internal audit functions. Only 15% of organizations' internal audit reviews viewed enterprise-critical third parties as one of the top areas of focus compared with 30% of regulatory bodies.

Broadly speaking, there is a large opportunity for internal audit reviews to better align with regulatory focus.

> "The regulators really cared about top-down oversight … They really cared about what are your top third parties that had the most impact, and do you have good oversight over them."
>
> **— Financial services executive**

During your organization's most recent regulatory body review, what were the two to three most important areas of focus?

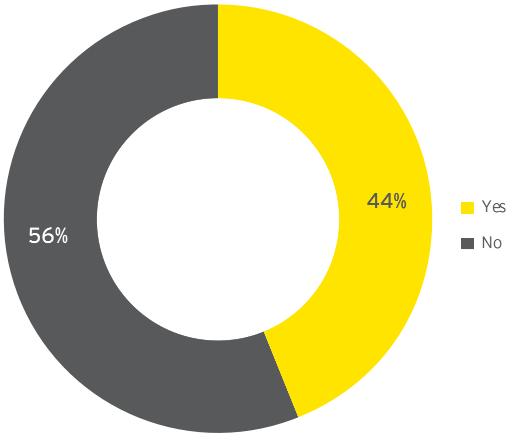
Most important areas of focus		
	Regulatory body	Internal audit
Inherent risk assessment	15%	21%
Onboarding activities	8%	13%
Enterprise-critical third parties	29%	15%
Oversight and governance	**42%**	**70%**
Fourth-party oversight	12%	6%
Operating models	8%	15%
Foreign-based third parties	2%	2%
Issue management and/or risk acceptance	10%	9%
Cybersecurity	**42%**	**30%**
Residual risk model	0%	2%
Maintenance of third-party inventory	10%	26%
Consumer protection	8%	2%
Privacy/confidentiality	9%	11%
Nontraditional third parties (e.g., brokers, agents, financial intermediaries)	4%	2%
Our program has not yet been assessed by a regulatory body	17%	4%

Multiple third-party cyber breaches are commonplace

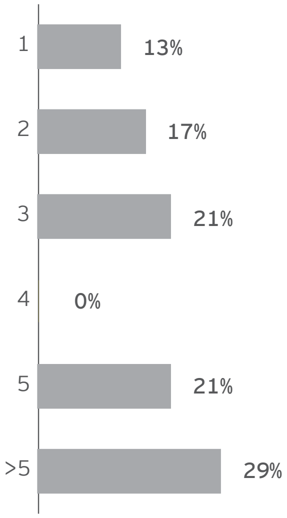
About half of organizations have either experienced a data breach or outage caused by a third party. Cybersecurity breaches and outages are relatively common among organizations surveyed, and when an organization has one breach or outage, it is likely that they have multiple. In fact, three-quarters (or more) of organizations that have one third-party breach or outage typically have multiple breaches or outages that are caused by third parties.

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

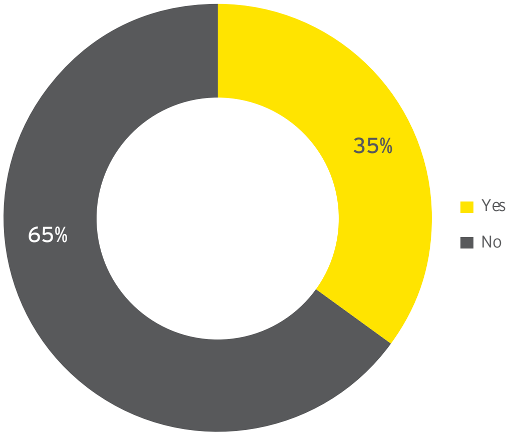
Data breaches caused by third parties



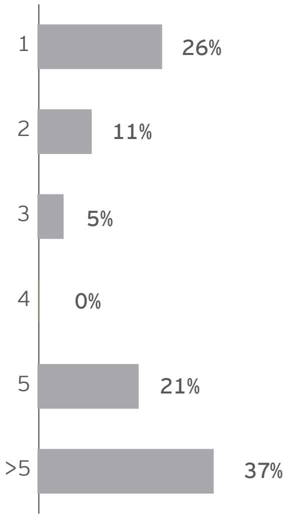
Number of issues



Outages caused by third parties



Number of issues



Industry alliances — growing trend may disrupt and shift perspectives on TPRM

At a glance

- Of entities surveyed, 44% have considered using an alliance or consortium to obtain efficiencies in certain areas. Of the 44%, 75% consider using an alliance for a common assessment framework, 58% for a common assessment service provider, and half have considered using common assessment resources.

Organizations seek efficiencies through alliances

Nearly half of organizations are considering the use of an alliance to drive efficiency in many aspects of TPRM. The most common area for an alliance is to achieve a common assessment framework. Additionally, 6 out of 10 organizations would consider using a common assessment provider, and 5 out of 10 favor the idea of leveraging common assessment resources employed by the alliance.

The strong interest in industry alliances represents a new trend in the market. In the past, alliances have been attempted without success; however, there are now active alliances with varying structures and value propositions that have the support and resources of some of the most mature financial services organizations and service providers in the industry. These alliances have the potential to disrupt how the industry manages third-party risk.

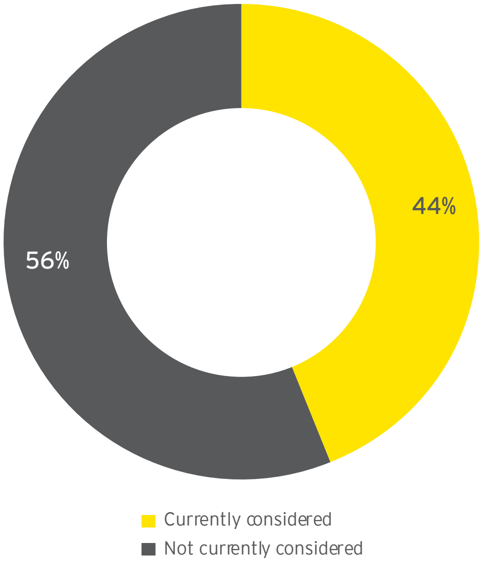
Should any alliance prove successful, organizations will be able to reduce costs and risk exposure by leveraging common frameworks and potentially sharing the results of what used to be proprietary and duplicative efforts within the market. Shifting the focus from transactional activities will enable leaner teams to focus on supporting and educating business partners and enhancing oversight and governance of third-party risks and management of issues.

An alliance model will also reduce the burden on third parties. As more financial services firms adopt the model, fewer unique assessments will need to be performed. This will allow third parties to be more efficient, reduce costs and potentially pass some of those savings on to the firms that engage them.

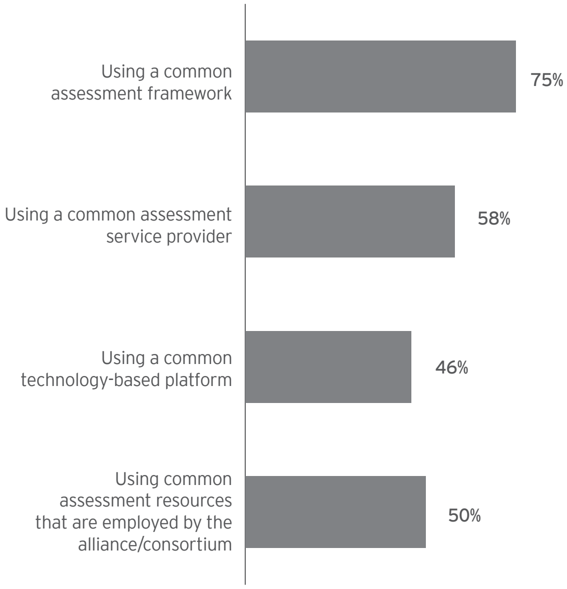
> "I would say our strategic focus is really on leveraging the alliance that we talked about. It will be about leveraging [a common] technology to support our management activities."
>
> **— Global banking executive**

Is your organization involved in an alliance or consortium seeking to obtain efficiencies in one or more of the following areas?

Involved in an alliance or consortium to obtain efficiencies in certain areas



Areas currently being considered



Assessment framework and regulations — moving towards standardization

At a glance

- Nearly three-quarters (72%) of organizations are using industry-standard questionnaires or have built their questionnaires by using a standard as a baseline, up from 44% in 2016. Fewer organizations (28%, down from 46%) are using completely proprietary questionnaires for third-party assessments.
- Most (83%) organizations assess compliance pre-contract for third parties that expose the organization to regulatory risk, up from 71% in 2016. In addition, 46% assess individual transactions post-contract for consumer compliance.

> "We're looking to go towards an industry standard, like a shared assessment. Some of the products and tools we're looking at are based on that shared assessment, on the SIG and the SIG Light. A couple of reasons why, it offers consistency and helps speed up the reviews. Secondly, if you're not using a standard questionnaire set that's kind of been vetted in the industry, people may interpret your questions differently than what you intended. So a lot of times you get just bad answers, because folks are trying to figure out what you're really asking them."
>
> **— Large insurance organization executive**

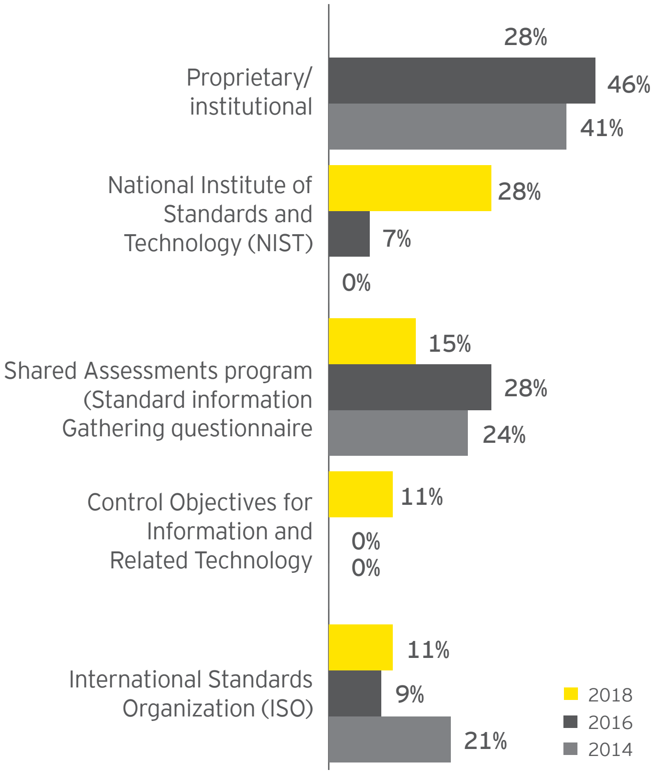
Standard questionnaires widely used

Around three of every four organizations (72%) use industry-standard questionnaires or have built questionnaires by using a standard as a baseline. This is up from 44% in 2016. And only 28% of organizations are using completely proprietary questionnaires for third-party assessments, which is down from 46% in 2016.

Setting industry standards seems to have been more difficult for the financial services community as many efforts have been started, yet very few have found long-term success. Adoption will take alignment among top 10 organizations within each sector, paving the way for broader adoption. The strong interest in industry alliances represents a new trend in the market. In the past, alliances have been attempted without success; however, there are now active alliances with varying structures and value propositions that have the support and resources of some of the most mature financial services organizations and service providers in the industry. These alliances have the potential to disrupt how the industry manages third-party risk.

What is the primary guidance used as a baseline for your control self-assessment questionnaire?

Primary guidance for self-assessment questionnaire



The lower the risk of the third party, the less often organizations perform control assessments on them. For the highest-risk third parties, control assessments are typically done annually. The majority of medium-rated third parties are assessed every two years, while almost all low-rated third parties are assessed more than every two years, or never assessed. This continues a trend we have seen over the past decade.

How often does your organization perform control assessments for your third parties based on risk posed to the organization?

Frequency of control assessments based on risk

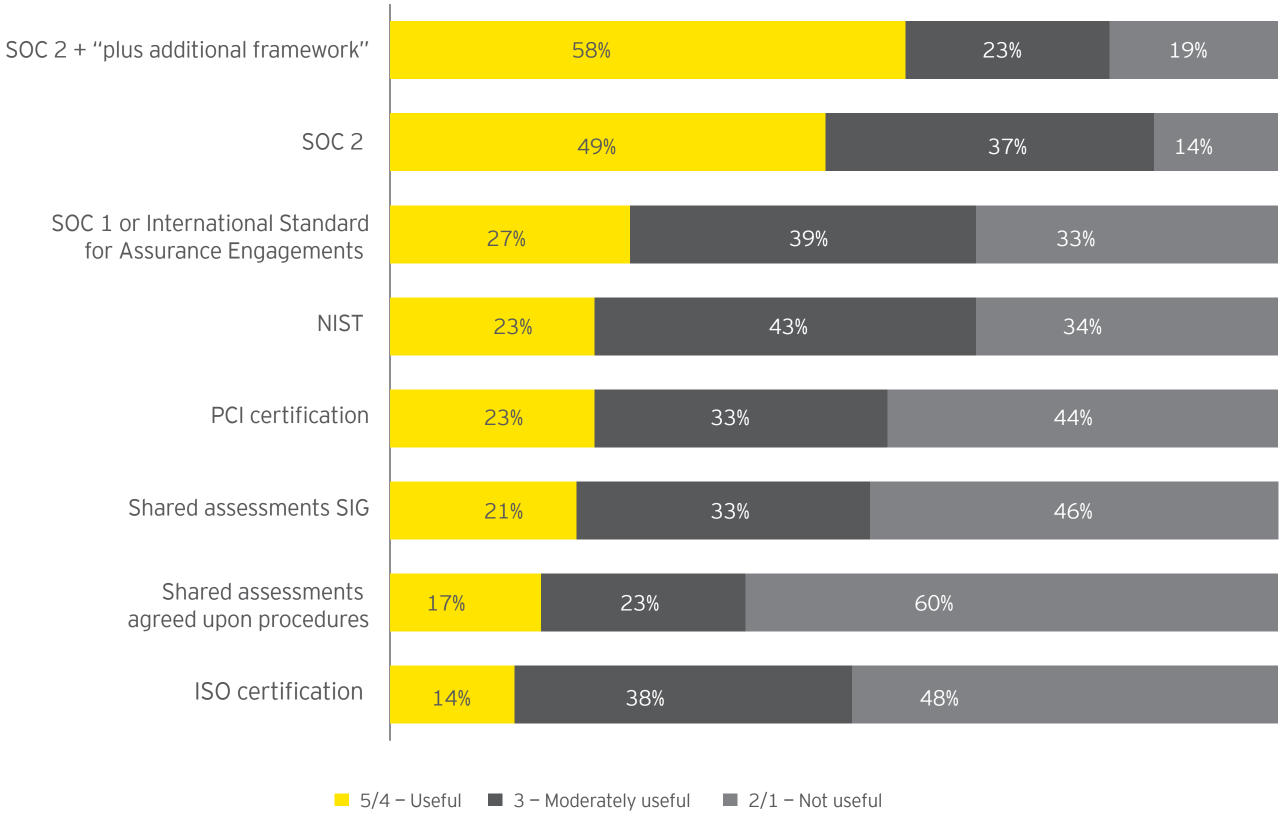
	Every 6 months	1 year	2 years	Less often than every 2 years
Highest risk	7%	**82%**	7%	4%
Medium risk	2%	21%	**56%**	21%
Lowest risk	0%	8%	11%	**81%**

More reliance on independent reviews

Organizations collectively believe that industry frameworks are useful in reducing or removing the need to perform a third-party review. SOC reports on their own, or combined with other frameworks, have been found to be the most useful in reducing the need to independently assess the risk of third parties, and organizations are relying on SOC more than they have in prior years. In fact, there was an increase to 86% of respondents finding the SOC 2 to be useful in 2018 vs. 71% in 2016. Reliance and usage of the other frameworks have remained relatively static over time.

On a 5-point scale, with 1 — not at all useful and 5 — extremely useful, when considering the need to perform a control review, which of the reports listed below are the most useful in reducing or removing the need to review a third party?

Usefulness of Industry Standard Compliance Reports



Greater efficiencies in on-site control assessment

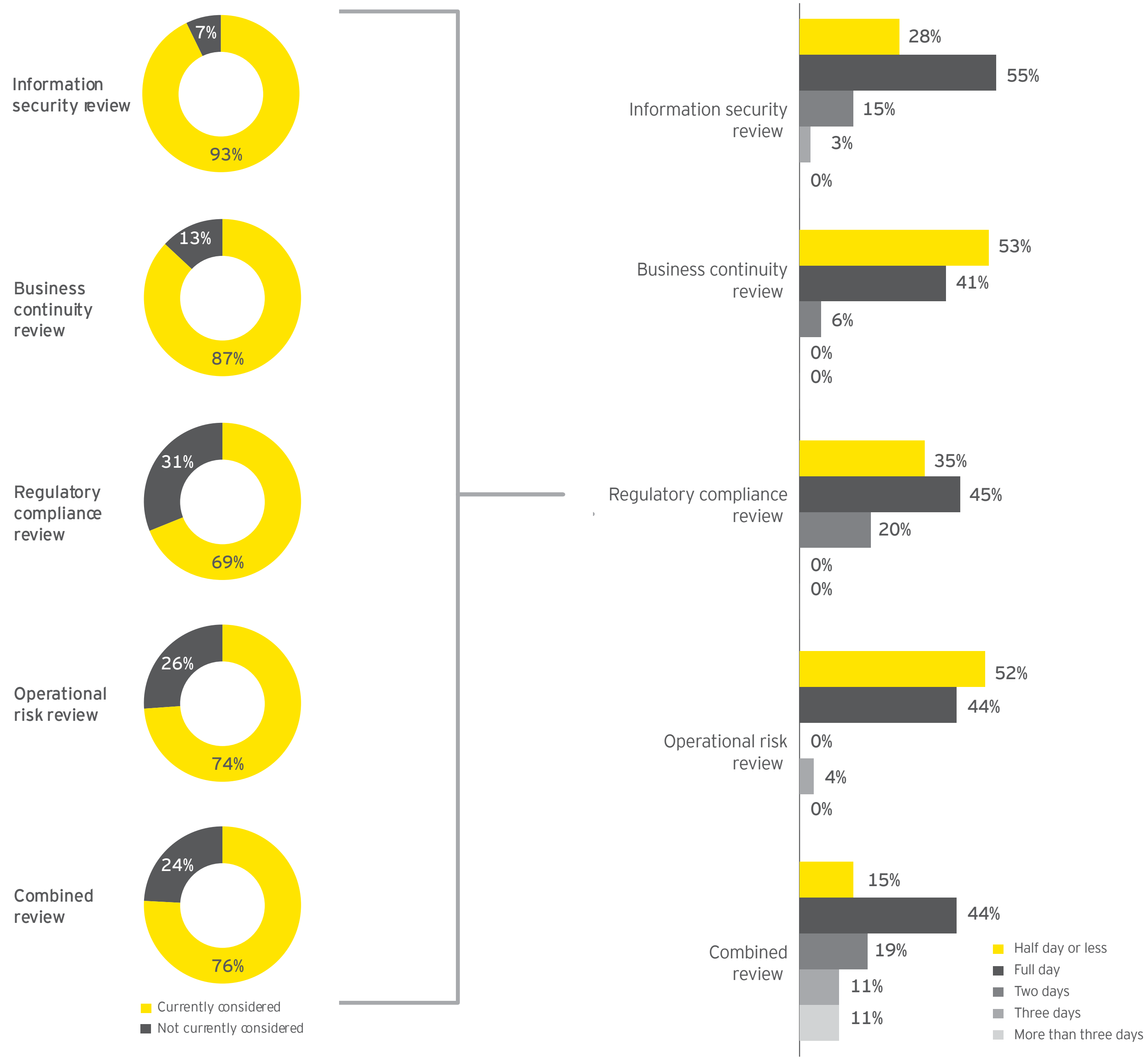
When assessing the four major risk domains — information security, business continuity, compliance and operational risk — 8 in 10 organizations reported spending at most one day on site to execute the review.

For combined reviews, 6 in 10 organizations typically complete them in 1 full day, but 40% of them required 2 days or longer to complete. As compared to 2016, however, the proportion of organizations spending 2 or more days on site for the combined review has decreased a bit, but organizations continue to grapple with the depth of the effort related to assessments where more than one risk domain is involved. The consolidation of assessment efforts across risk domains does, however, point to the fact that organizations are looking to become more efficient in the operational assessment functions.

When conducting an on-site review at a third-party site, what is the typical duration of the site visit for each of the following components of the review (excluding travel)?

Conducting on-site reviews

Duration of on-site reviews

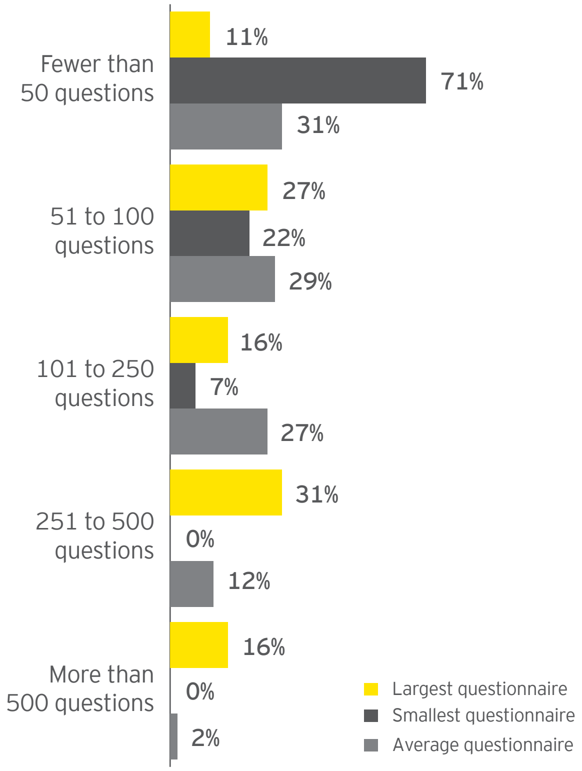


Longer questionnaires reflect risk consolidation

Almost 50% of organizations reported using questionnaires that are longer than 250 questions. With the rise in questionnaire content depth and the nominal changes in duration of standard assessments, a conclusion can be made that either organizations are looking at more, but not going as deep, into the validation or the increases are driven by consolidating other risk domains into a single effort. We think the latter is more likely.

> "I think there is a balance between getting to the amount of information that you really need to do the appropriate level of due diligence and expect or put forward what needs to be mitigated in order to engage with that third party, versus burdening."
>
> – Global financial services executive

How many questions are within your organization's control self-assessment questionnaires that are used to assess the third parties?



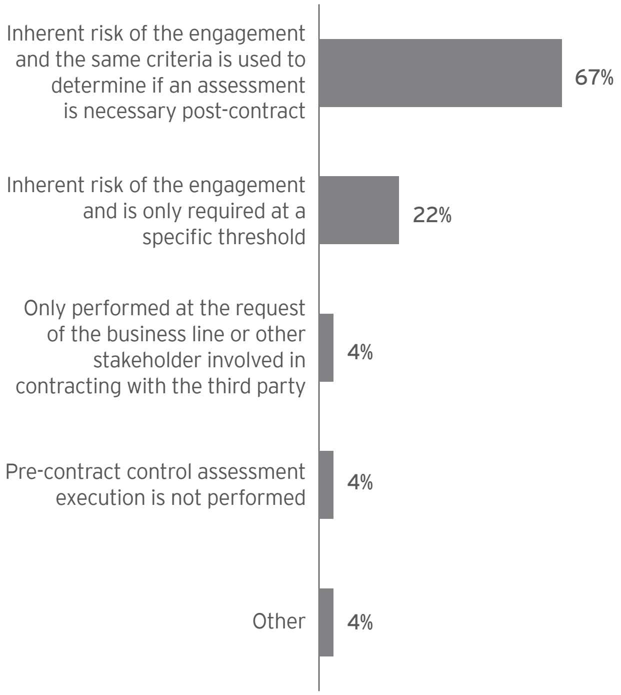
Rightsizing due diligence indicates maturity

Three-quarters of organizations surveyed noted that they apply the same level of depth to pre-contract due diligence assessments as they do to their post-contract control assessments. However, organizations with more mature risk management programs have found that they can use a lighter touch during due diligence. Using maturity as a key indicator, we would expect rightsizing due diligence to be a key focus for organizations on the middle to lower end of the maturity spectrum. We also feel this is a significant factor in the end-to-end time frame for execution of contracts and could be a significant source of cycle time cost takeout for many organizations. This may also be an area where efforts around market utilities can present quick access to data to make pre-contraction decision-making much more efficient for lower-risk suppliers.

Nearly all (90%) organizations also noted that they completed pre-contract due diligence where the inherent risk rating was high, pointing to a heavier focus pre-contract on higher-risk services and third parties.

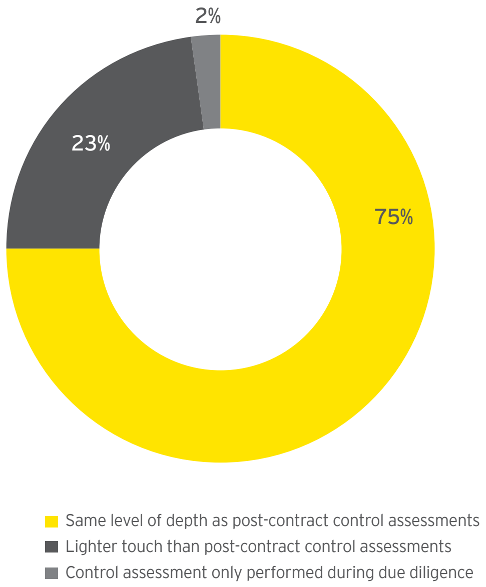
What is the primary driver of conducting pre-contract due diligence control assessments?

Primary driver of pre-contract due diligence control assessments



What level of depth of assessment is performed when conducting pre-contract due diligence control assessments?

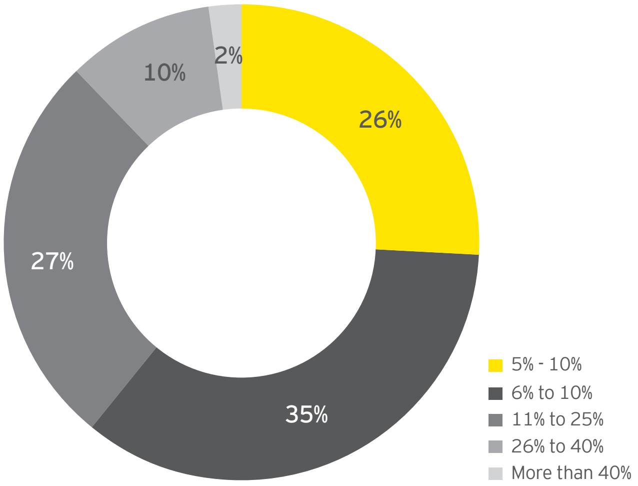
Primary driver of pre-contract due diligence control assessments



Compliance assessments often continue post-contract

Most (88%) organizations reported that fewer than 25% of in-scope third parties expose the organization to regulatory risk. A large majority (83%) have been successful in implementing tactics to prevent exposure to regulatory risks prior to the contracting phase with these third parties. A large amount of those firms (67%) continue the assessments post-contract, while almost half (46%) perform individual transaction assessments on a more tactical basis to ensure compliance, a similar proportion as two years ago.

What percentage of third parties in scope for risk monitoring expose the organization to regulatory risk, specifically consumer compliance?



When are regulatory compliance reviews conducted? Please select all that apply.

When regulatory reviews are conducted		
	Compliance control assessments	Individual transaction assessments
Pre-contract	**83%**	13%
Post-contract	67%	**46%**
Not performed	7%	15%
Not applicable	2%	11%

Industry outlook — top areas for investment

At a glance

- In response to the challenges reported in the survey around governance and reporting, 94% of organizations plan to spend more or the same on third-party risk technology enablement during 2018.

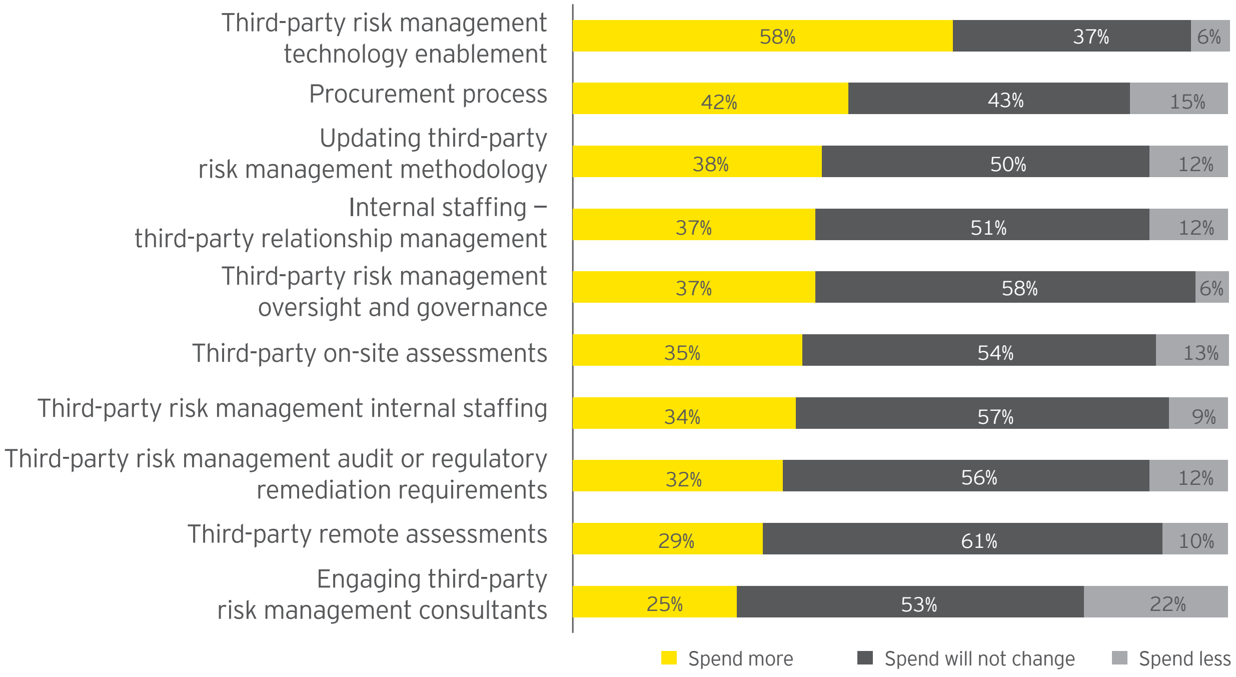
Compared to the current year, does your organization plan to spend more, less or the same amount for the following activities?

Investment in TPRM set to increase

While TPRM program maturity continues to increase across the industry, 6 out of 10 firms are planning on spending more in 2018 on TPRM technology enablement. This is up from 5 out of 10 firms in 2016.

As TPRM programs continue to mature, spending allocated to TPRM oversight and governance, TPRM audit and remediation requirements, and TPRM methodology all will see spending increase, as 9 out of 10 organizations plan on investing just as much if not more in these areas in 2018 as they did in 2016.

Spending in the future



Demographics

Between October and December of 2017, EY surveyed 54 global financial services organizations with third-party risk functions of varied maturity and sizes, primarily across banking and capital markets, insurance, and asset management. The purpose of the survey was to address the distinctive nature of managing third-party risk in the financial services industry.

Of the companies surveyed, 63% had fewer than 25,000 employees and 26% had more than 50,000 employees, a major change from last year's survey, where over half the firms were 50,000 or more. Of those surveyed, over half had third-party risk management programs in place for more than five years, 15% for three to five years and ~30% for fewer than three years.

Respondent profile		
Total	**54**	
By industry	**# of respondents**	**%**
Banking and capital markets	34	63%
Insurance	12	22%
Asset management	6	11%
Other*	2	4%
Program operation lifetime		
Fewer than 3 years	16	29%
Between 3 and 5 years	8	15%
More than 5 years	30	56%
By company size		
Fewer than 25,000	34	63%
25,001 to 50,000	6	11%
50,001 to 100,000	8	15%
More than 100,000	6	11%

Our 2018 survey had 54 respondents, up from 49 in 2016. 36 of these respondents conduct primary business operations outside of the US, or have a footprint in both the US and abroad and the remaining have US only operational footprints. Amongst the Financial Institutions that participated, the geographic representation is as follows: Australia (2), Asia-Pacific (3), Japan (1), North America (36) and Europe (12). The survey was conducted between October and December of 2017.

Contacts

Matthew Moog
Principal, Ernst & Young, LLP, Financial Services Advisory
New York
Matthew.Moog@ey.com
+1 347 225 2261

Michael Giarrusso
Partner, Ernst & Young, LLP, Financial Services Risk Advisory
Boston
Michael.Giarrusso@ey.com
+1 617 585 0395

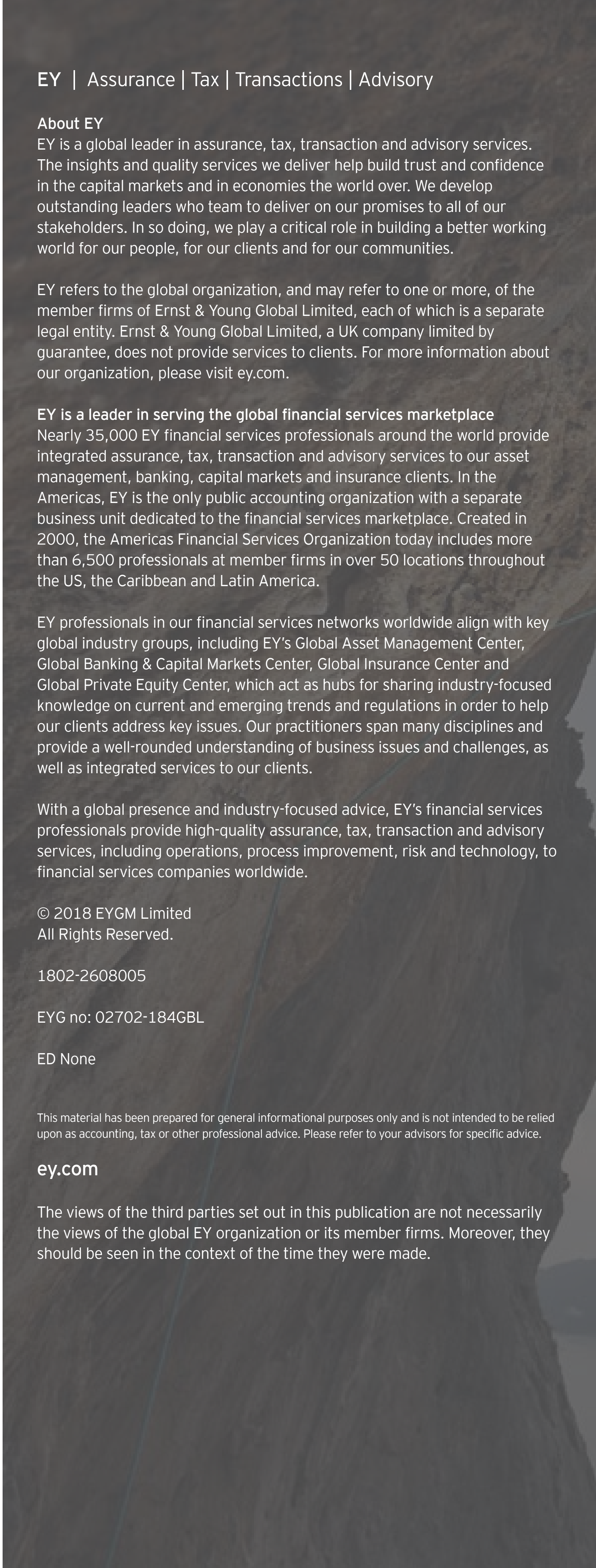
Chris Ritterbush
Executive Director, Ernst & Young, LLP, Financial Services Risk Advisory
Houston
Chris.Ritterbush@ey.com
+1 713 562 0999

Kanika Seth
Partner, Ernst & Young, LLP, EMEIA Financial Services
London
Kseth@uk.ey.com
+447500975272

Chris Lim
Partner, Ernst & Young Advisory Pte. Ltd, Financial Services Risk Advisory
Singapore
Chris.Lim@sg.ey.com
+65 6309 6320

Harald deRopp
Executive Director, Ernst & Young, LLP, Financial Services Risk Advisory
Japan
Harald.deRopp@jp.ey.com
+81 3 3503 1110

Hanny Hassan
Partner, Ernst & Young, Financial Services Risk Advisory
Australia
Hanny.Hassan@au.ey.com
+61 421 201 317



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. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 35,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 6,500 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services networks worldwide align with key global industry groups, including EY's Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

1802-2608005

EYG no: 02702-184GBL

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

The views of the third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.