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

EY Global Third-Party Risk Management Survey 2019–20

Financial services sector survey results

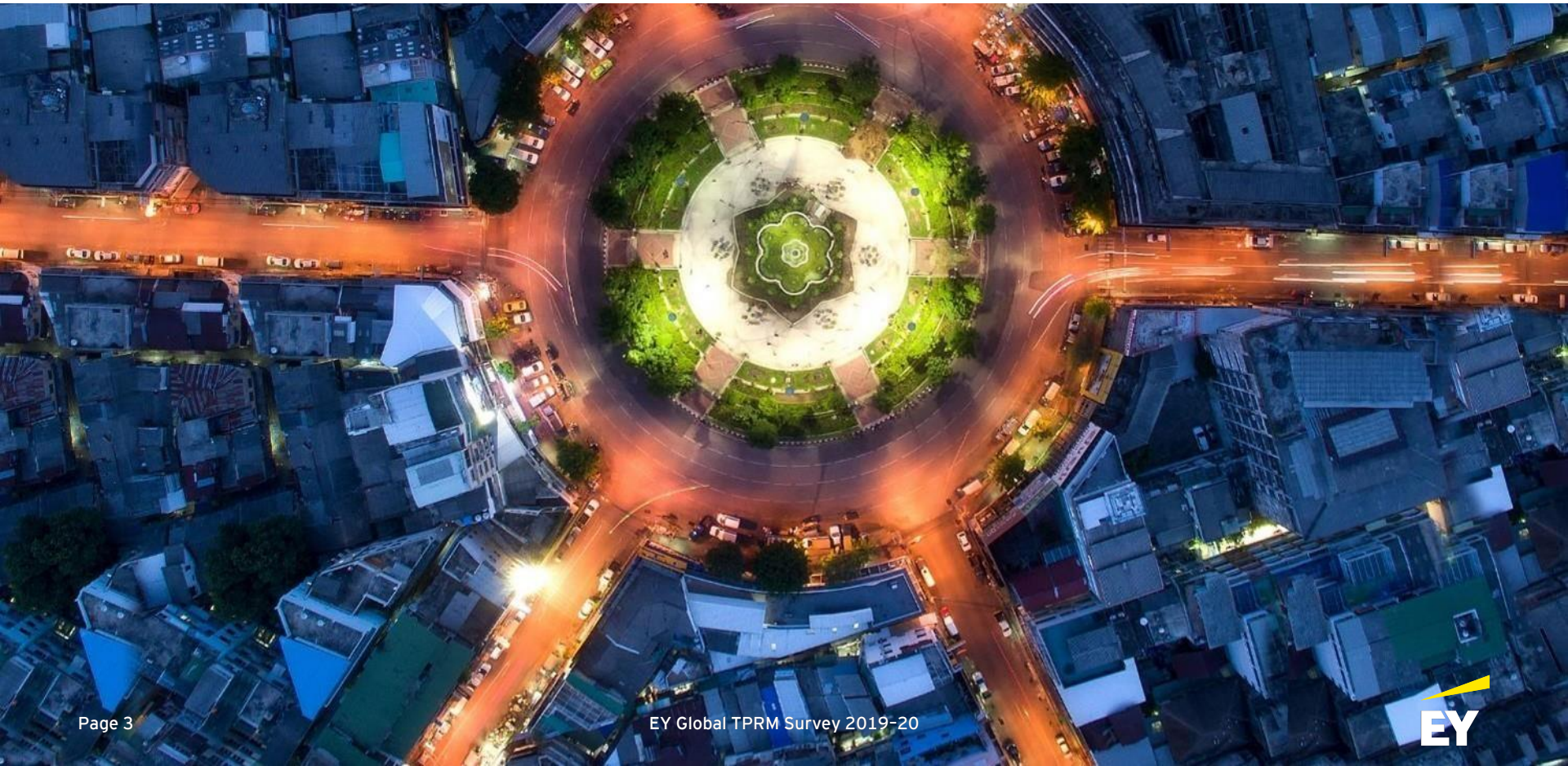
EY
Building a better working world

Disclaimer

- 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.
-
- These slides are for educational purposes only and are not intended, and should not be relied upon, as accounting advice.
- Percentages are shown as whole numbers. As a result, some percentages may not sum to 100%.

Table of contents

Financial services sector results



Background

From July to September of 2019, EY professionals conducted a survey of 246 organizations (including 123 financial services organizations) of various sizes and maturity levels from around the globe and across a variety of industries. Although the executives who completed the survey were from various functions within each organization, all functions had a role in third-party risk. These functions included, but were not limited to, enterprise risk management, procurement, cybersecurity, internal audit and finance. The purpose of the survey was to address the distinctive nature of third-party risk across industries.

Industries in the overall survey included, but were not limited to, financial services, consumer products and retail, health care, life sciences, media and entertainment, technology, power and utilities, diversified industrial products, and the government and public sector. The results in this document only include responses from financial services organizations encompassing firms in banking and capital markets, insurance, and wealth and asset management.

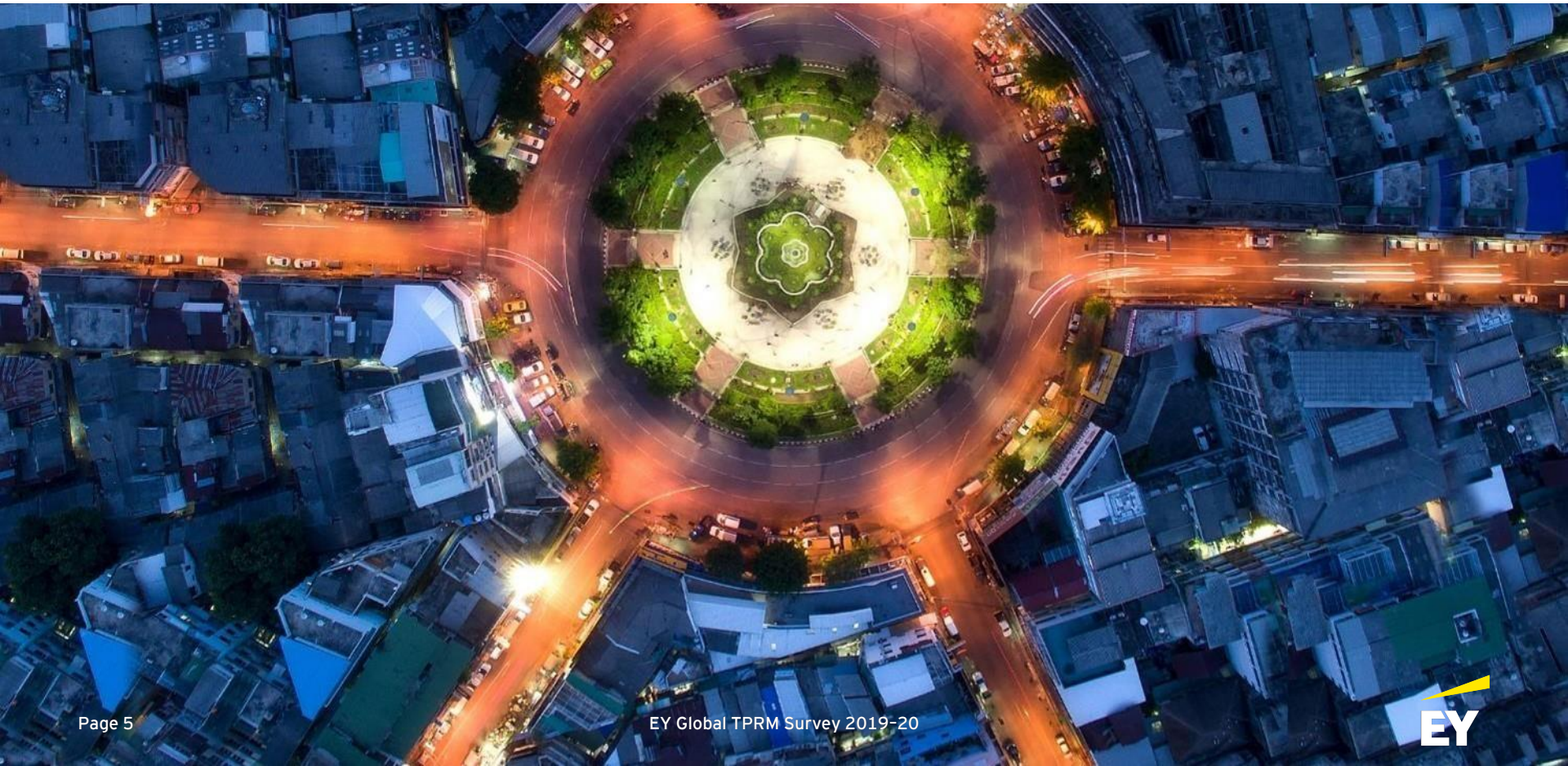
In this survey, we asked participants to respond to questions within several key areas of their respective third-party risk management (TPRM) programs. Topics included:

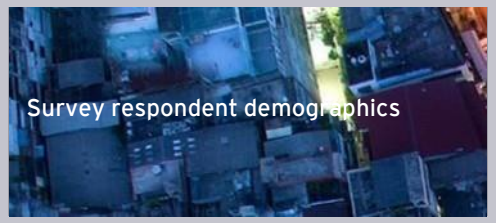
- TPRM/function organization, governance and oversight
- Third-party population breakdown/risk tiering
- Assessments
- Issue management/risk treatment
- Fourth-party management
- Reporting
- Technology
- Cybersecurity and threat intelligence
- Inbound requests
- Privacy regulations
- Regulatory and internal audit exams
- Non-traditional third parties
- Concentration risks (financial services only)
- Affiliate management (financial services only)
- Innovation

This document includes the results aggregated for each question across respondents from the financial services industry.

For any questions, support for data interpretation or specific data requests, please reach out to tprm@ey.com.

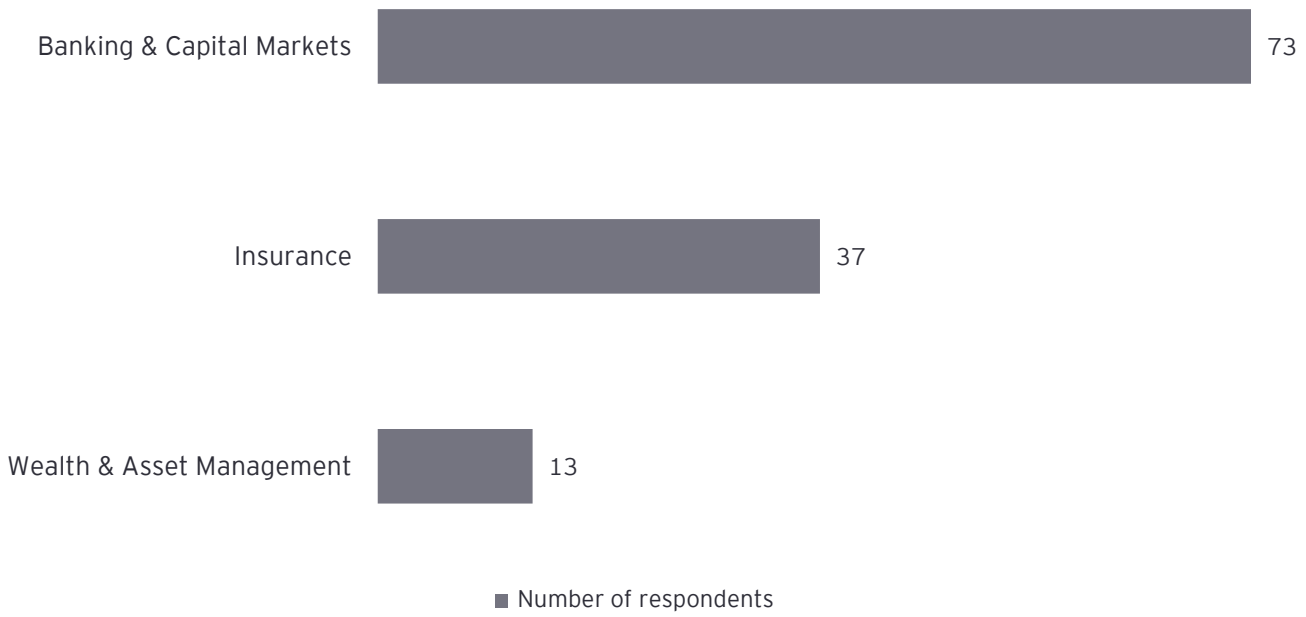
Survey respondent demographics

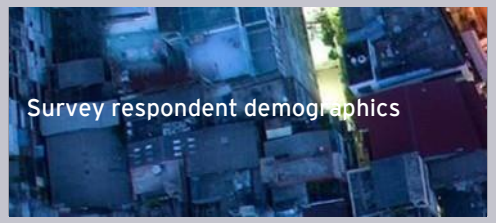




Of the 246 survey participants, the largest number of respondents came from the banking and capital markets sector, a result of the tenure of programs and regulatory pressures. Fifty percent, or 123 respondents, came from the financial services sector including banking and capital markets, insurance, and wealth and asset management.

Respondent profile (Q1) number of respondents

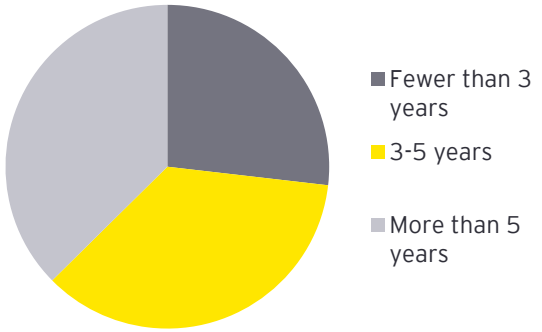




Over half of the financial services companies surveyed were in the Americas, more than one-third in Europe and the remainder in Asia-Pacific. The majority (73%) of organizations have had third-party risk management programs in place for three to five years or more than five years.

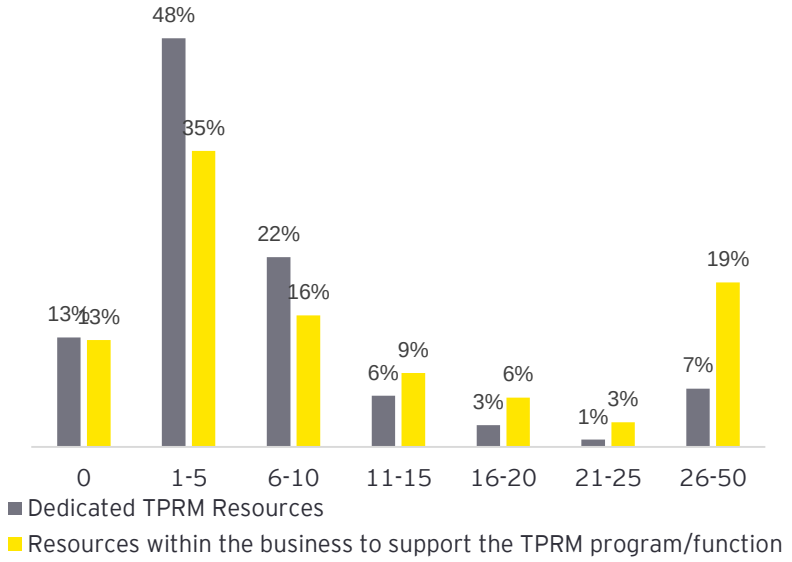
Respondent profile (Q2, Q3, Q4)	Participants	
By region	#	%
Americas	68	55%
Europe	46	37%
Asia-Pacific	9	7%
By company size (headcount)		
Fewer than 5,000	52	42%
5,001 to 15,000	30	24%
15,001 to 25,000	10	8%
25,001 to 50,000	13	11%
50,001 to 100,000	12	10%
More than 100,000	6	5%

TPRM program operation lifetime

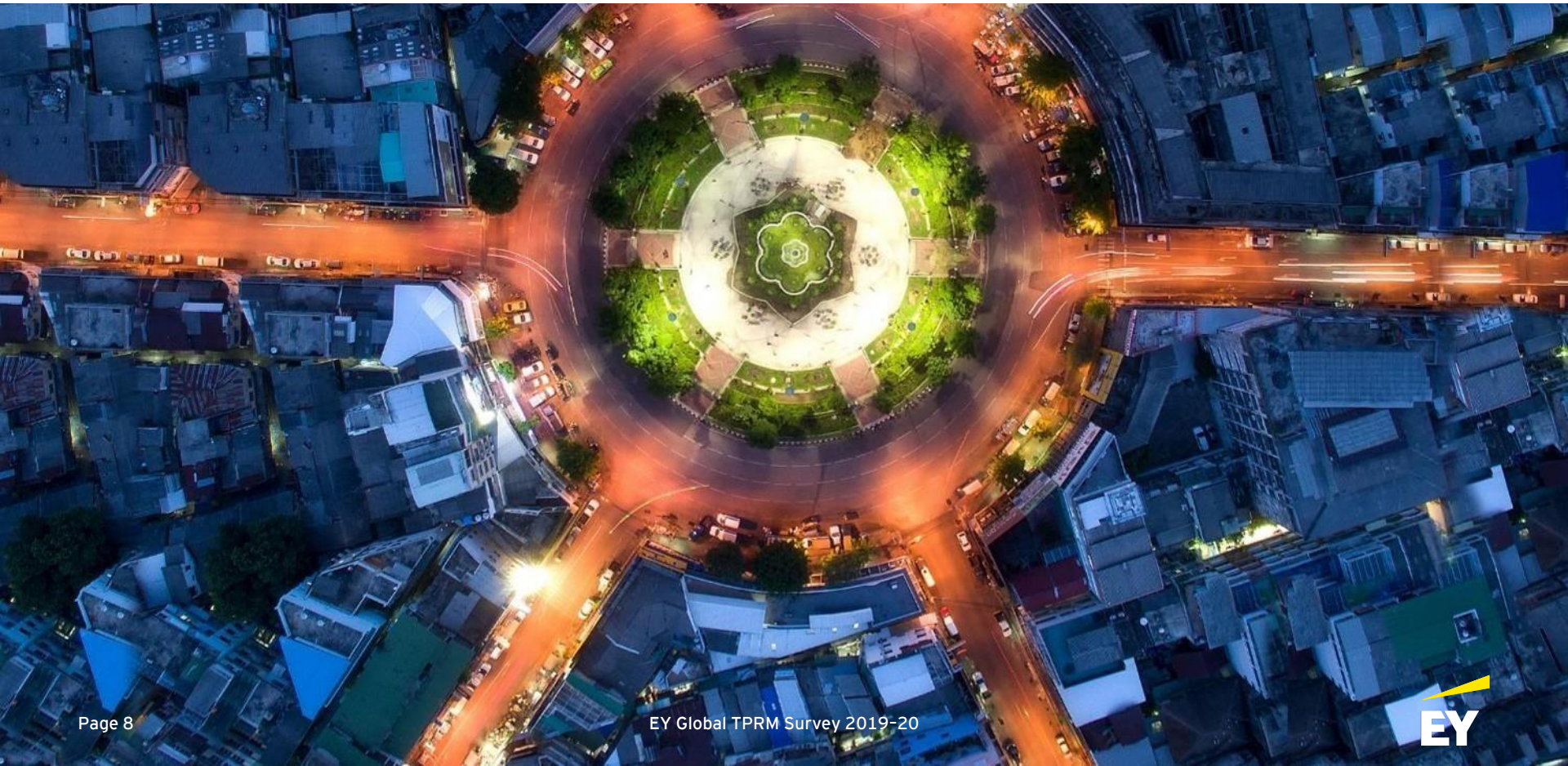


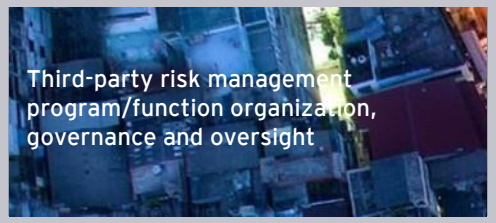
TPRM program resources

Q8. How many resources support your third-party risk management program/function in the following categories?



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

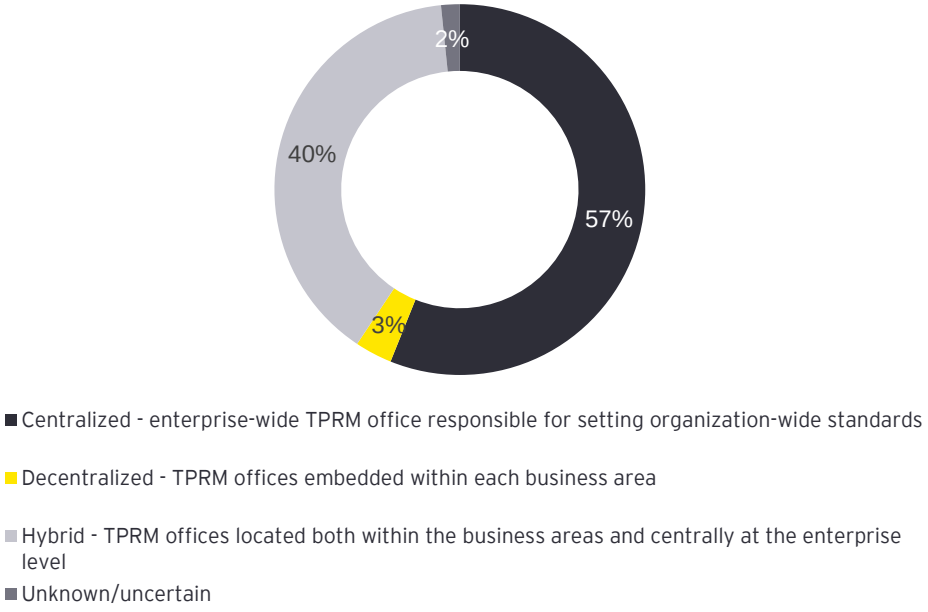




Centralized and hybrid models continue to be the most common structure for TPRM programs in the financial services industry, signifying the importance of a consistent, yet flexible, TPRM function at organizations with more stringent regulations. This figure is unchanged from last year; however, the 3% decentralized structure is down from 7% the previous year, suggesting that a hybrid model is becoming more common.

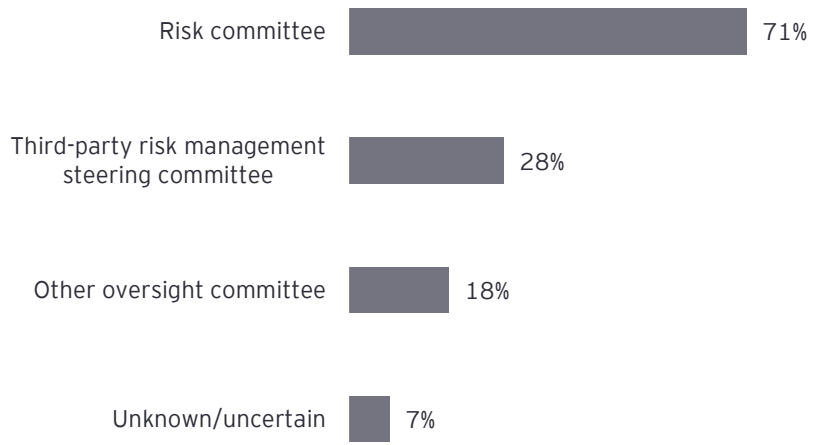
TPRM program structure

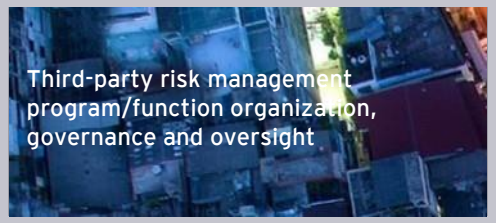
Q5. How is your third-party risk management program/function structured?



TPRM committee oversight

Q6. Which of the following committees oversees your third-party risk management program/function activities?

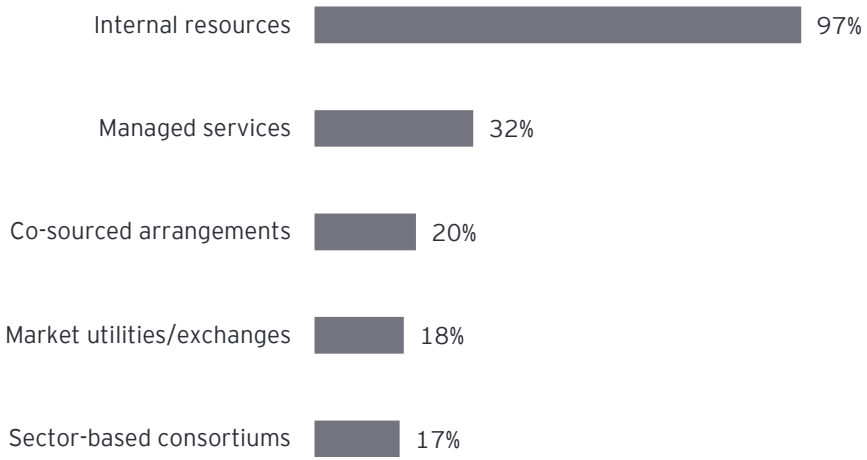




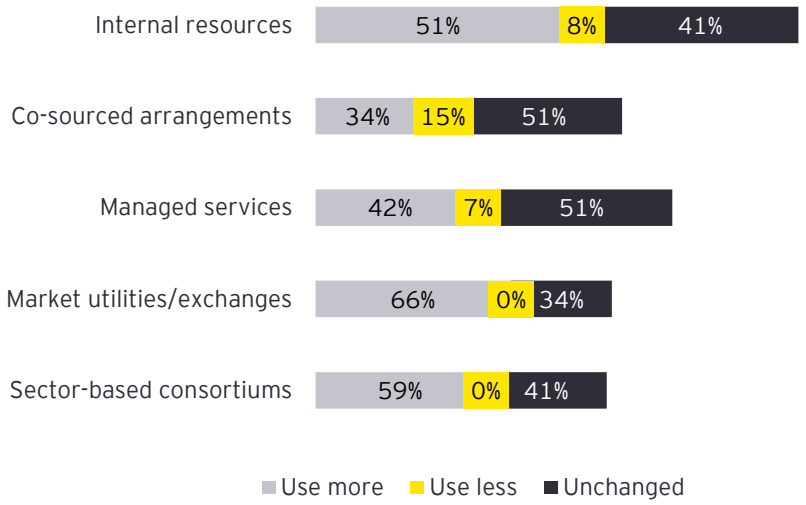
Looking out over the next two to three years, there is a desire among the organizations surveyed to leverage external solutions more actively. More than 40% of the financial services organizations surveyed expect to more frequently use managed service providers to execute their third-party risk management function; that figure jumps to more than 50% for sector-based consortiums and to more than 60% for market utilities.

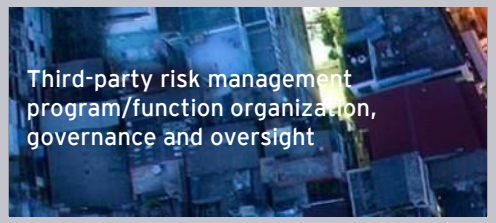
TPRM execution

Q7A. Does your organization currently use any of the following for the execution of your third-party risk management program/function?



Q7B. How do you expect that to change in the next two to three years?

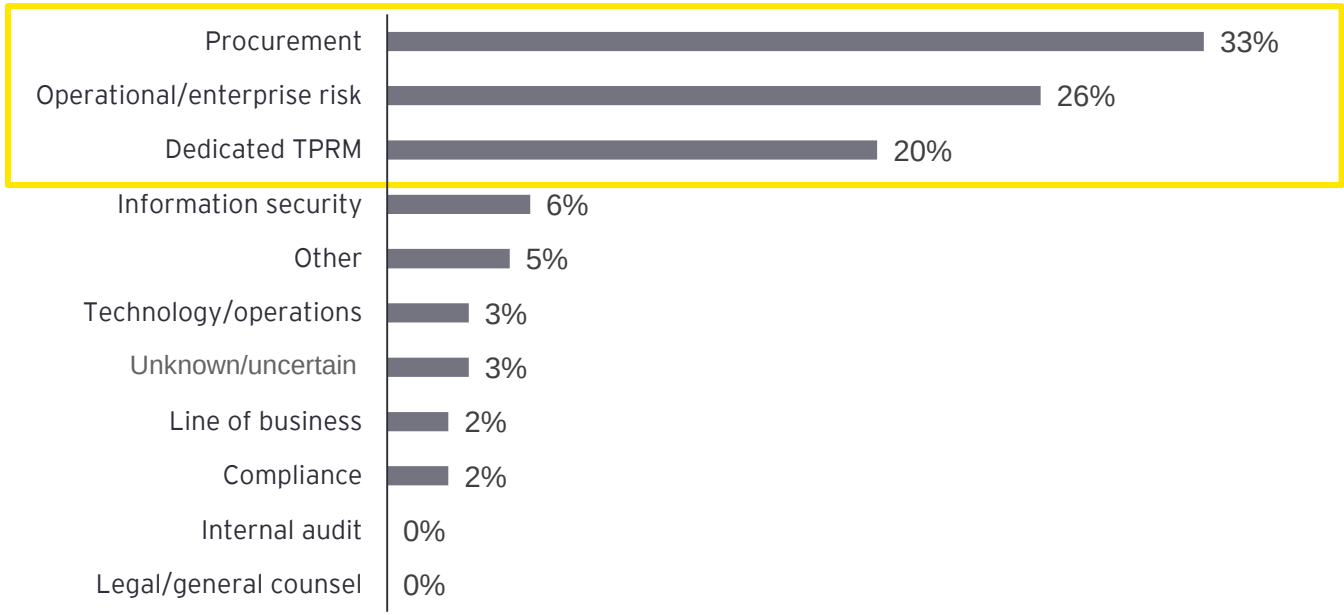


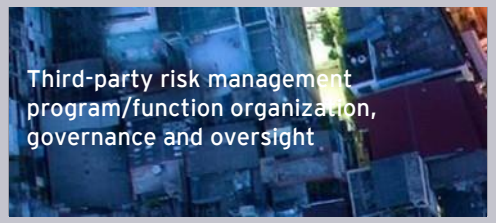


There is still no consensus across the financial services organizations surveyed as to who owns the TPRM function. Thirty-three present of respondents indicated that procurement has primary ownership, slightly down from the 37% from last year's survey. One in four survey respondents indicated that operational/enterprise risk owns it, and an additional 20% indicated they have a dedicated TPRM group that owns it.

Integrated with TPRM program

Q9. What area has primary ownership of the third-party risk management program/function?





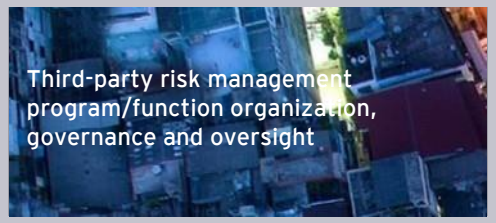
Across the financial services organizations surveyed, there is some consensus on procurement's ownership of third-party inventory management and contract expiration and termination. There is little consensus on ownership of risk-related activities.

TPRM functional area responsibility

Q10. Which functional area has primary responsibility for the execution of the following components of your organization's third-party risk management program/function?

Component	Procurement	Third-party risk management	Legal/ general counsel	Information security	Operational/ enterprise risk	Compliance	Line of business	Technology/ operations	Internal audit	Other	Not conducted
Third-party inventory management	42%	31%	1%	3%	10%	1%	7%	1%	1%	0%	1%
Design and facilitation of the inherent risk assessment process/framework	13%	30%	3%	15%	23%	7%	3%	3%	1%	2%	1%
Review and updating of contract terms as part of ongoing monitoring	30%	6%	30%	6%	2%	4%	16%	2%	1%	1%	3%
Identification of expired contracts	55%	5%	10%	0%	2%	1%	23%	1%	0%	1%	3%
Termination of contracts	41%	6%	19%	1%	1%	1%	27%	1%	0%	1%	1%
Issue management/risk treatment	4%	19%	3%	9%	21%	6%	30%	3%	2%	2%	3%

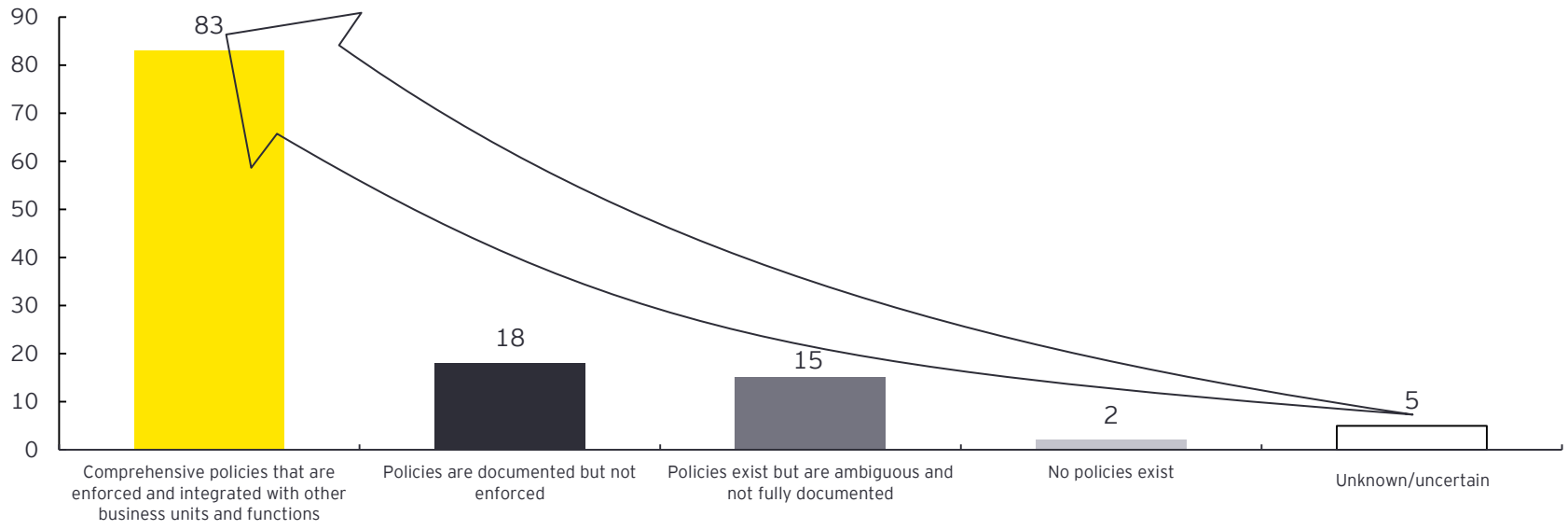
Note: Outlined percentages represent responses greater than 30%.



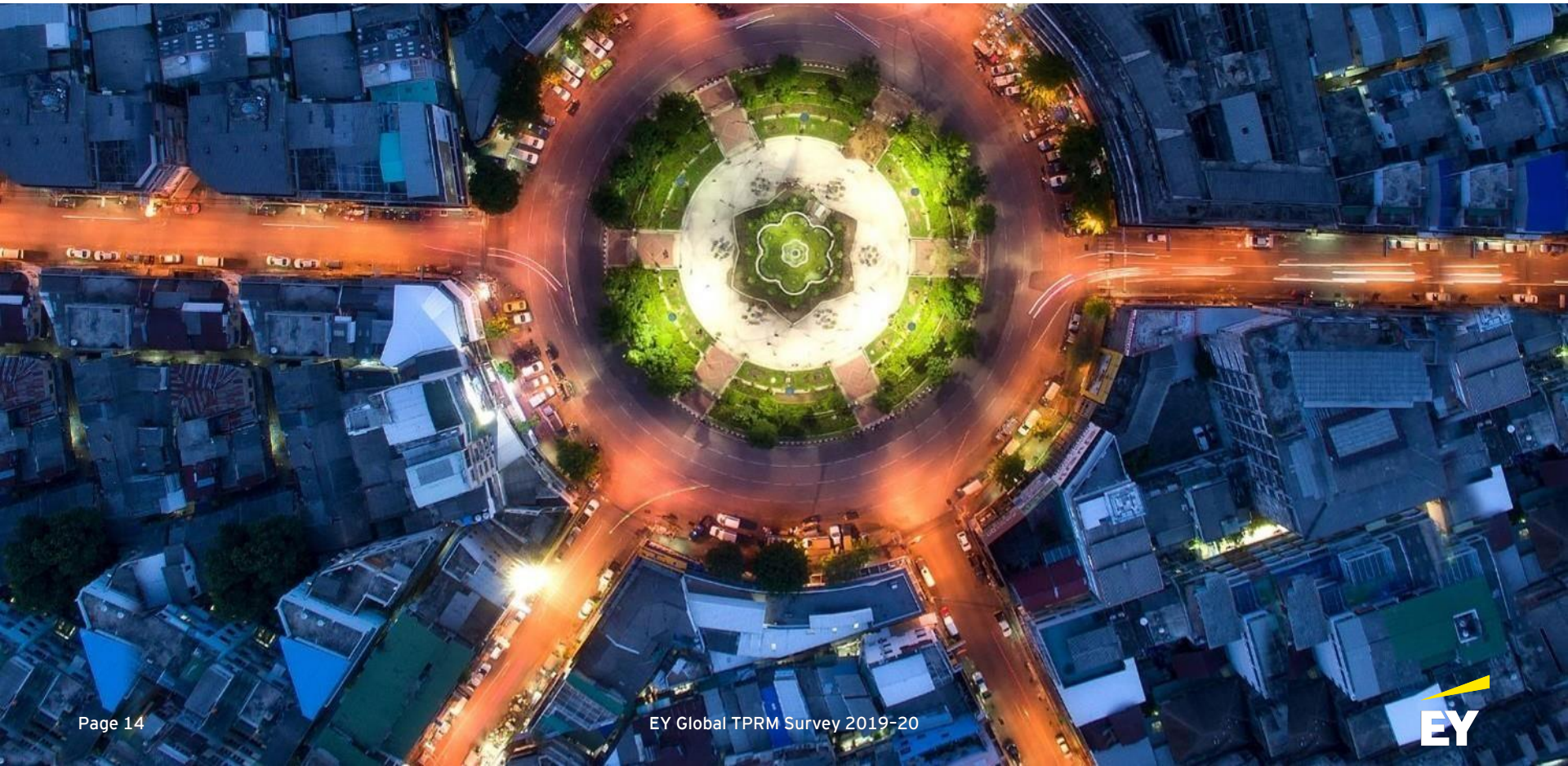
Over two-thirds of financial services organizations surveyed indicated they have comprehensive policies that are enforced and integrated; 27% indicated that policies are either documented but not enforced or exist but are not fully documented.

TPRM policy types

Q11. Which of the following best describes the policies your organization has in place to support your third-party risk management program/function?



Third-party population breakdown/risk tiering



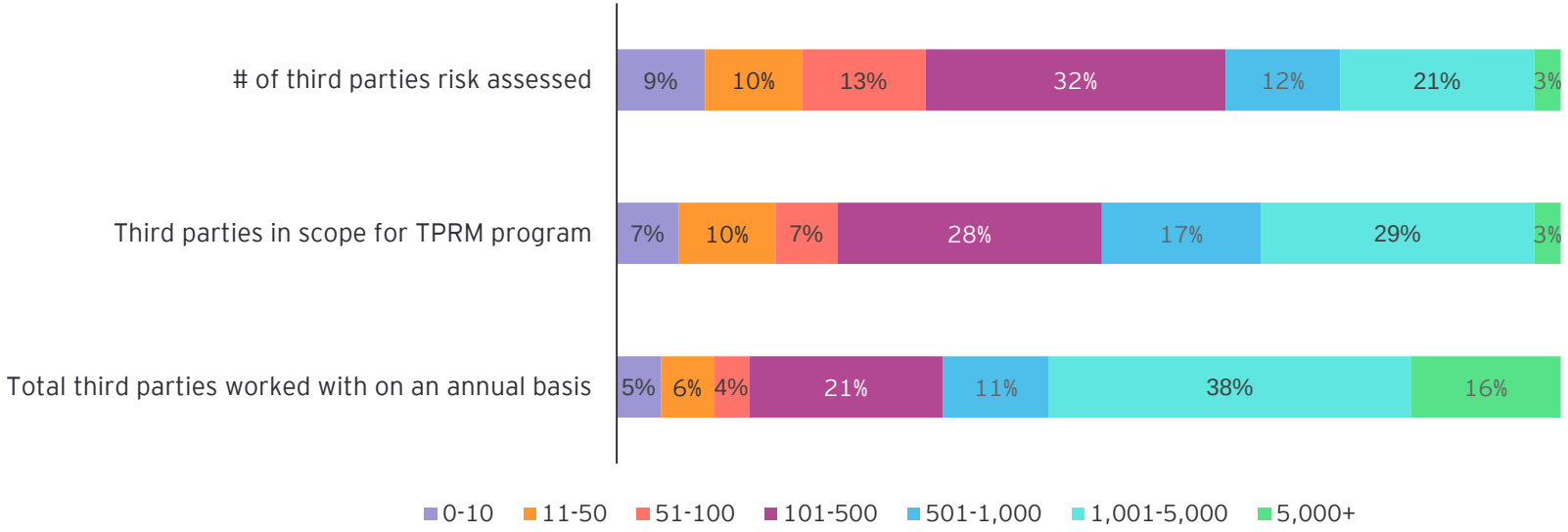
There is little consensus on the percentage of third parties subject to the TPRM program or a risk assessment, with the most common ranges being 101-500 and 1,001-5,000 third parties. Thirty-eight percent of organizations indicated that they work with 1,001-5,000 third parties on an annual basis. Interestingly, the third-party volume is related to the on-site vs. remote assessment percentages (Q39), as the more third parties an organization assesses, the fewer on-site assessments are executed as a percentage of total assessments.

Third-party volume

Q12. Approximately how many third parties does your organization work with on an annual basis?

Of the total number of third parties, approximately how many third parties are in scope for your third-party risk management program/function?

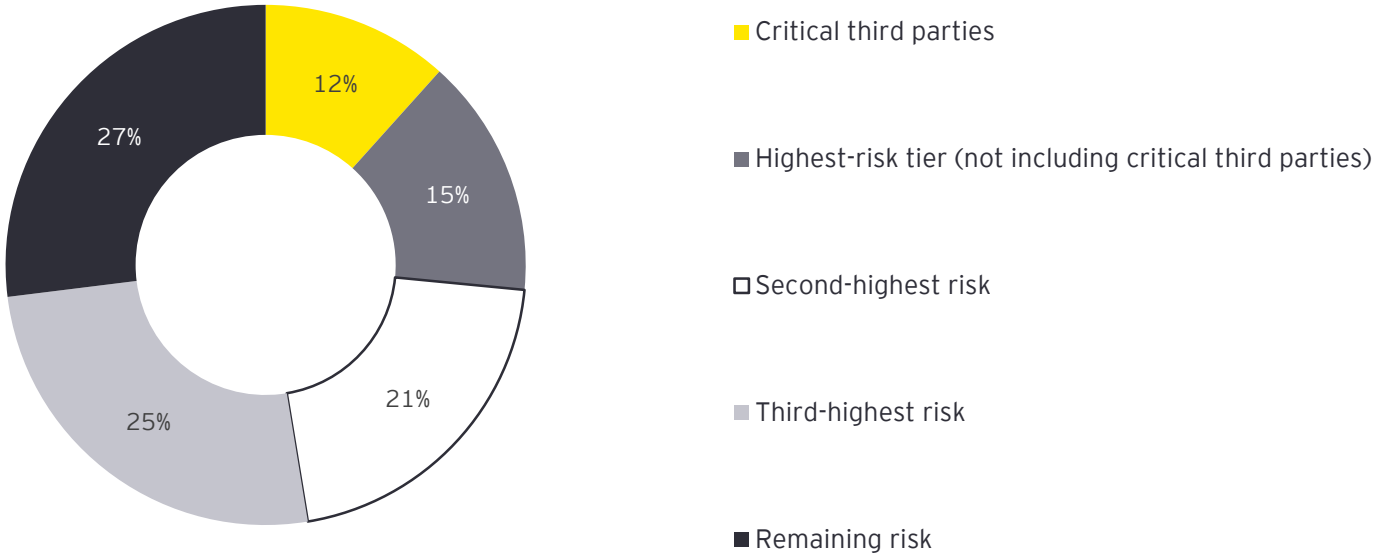
Of the total number of third parties in your program/function, how many have been risk-assessed?



Across financial services organizations surveyed, over one-quarter of third parties fall into the highest-risk tier and critical categories. The remaining third parties are spread across second-highest risk, third-highest risk and remaining risk categories.

Third-party risk scale

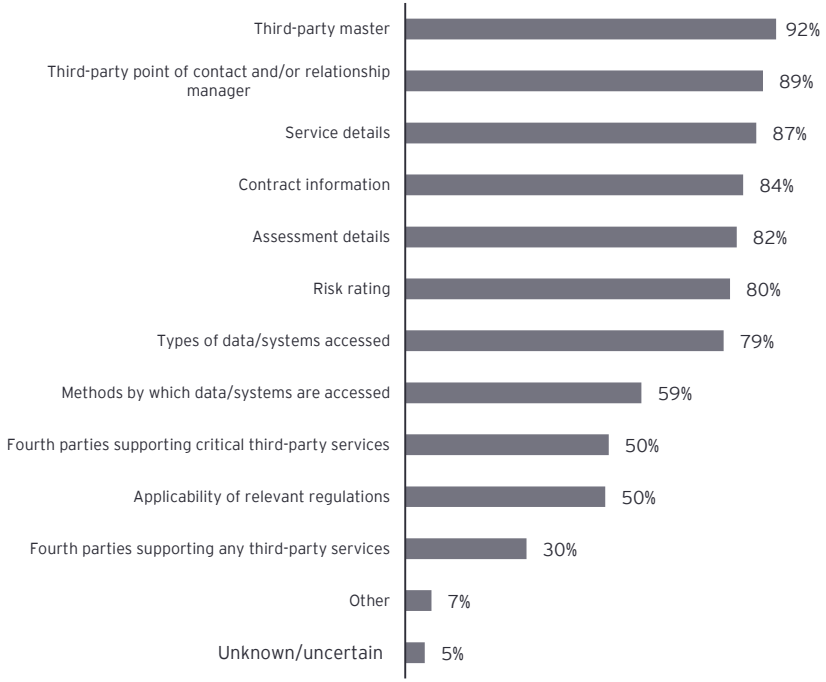
Q13. What percentage of third parties is in scope for your third-party risk management program/function in each of your organization's risk tiers/ranks? Total must equal 100%.



Over half of the financial services organizations surveyed indicated that both sensitivity of data and business continuity and resiliency are among the top three most important criteria used to define a critical third party. Strategic importance, type of data and systems accessed, and financial impact were among the next most important criteria, each chosen by about one-third of respondents.

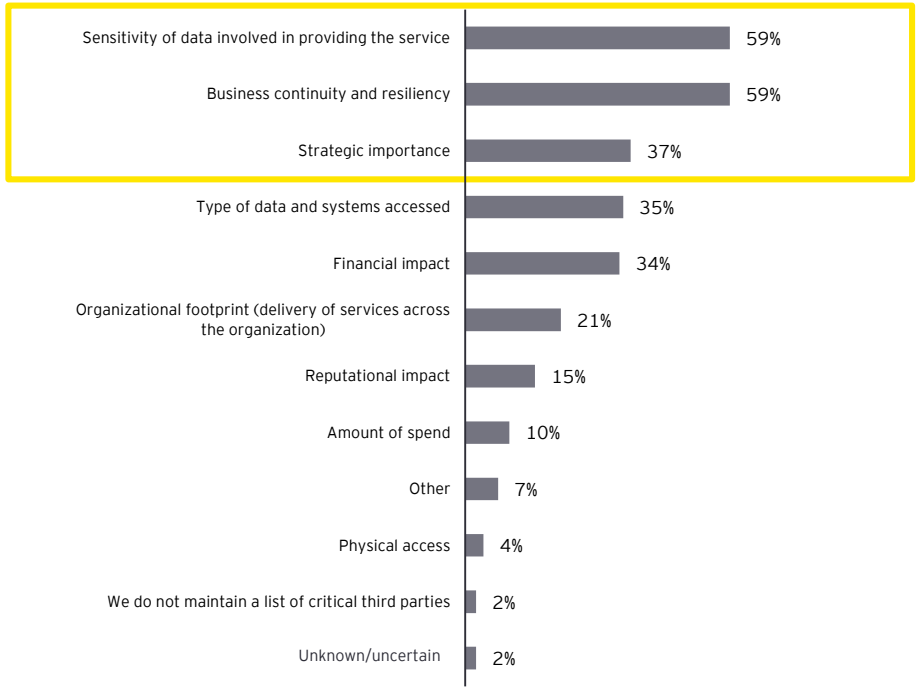
Information maintained

Q14. What types of information do you maintain with respect to your third parties?

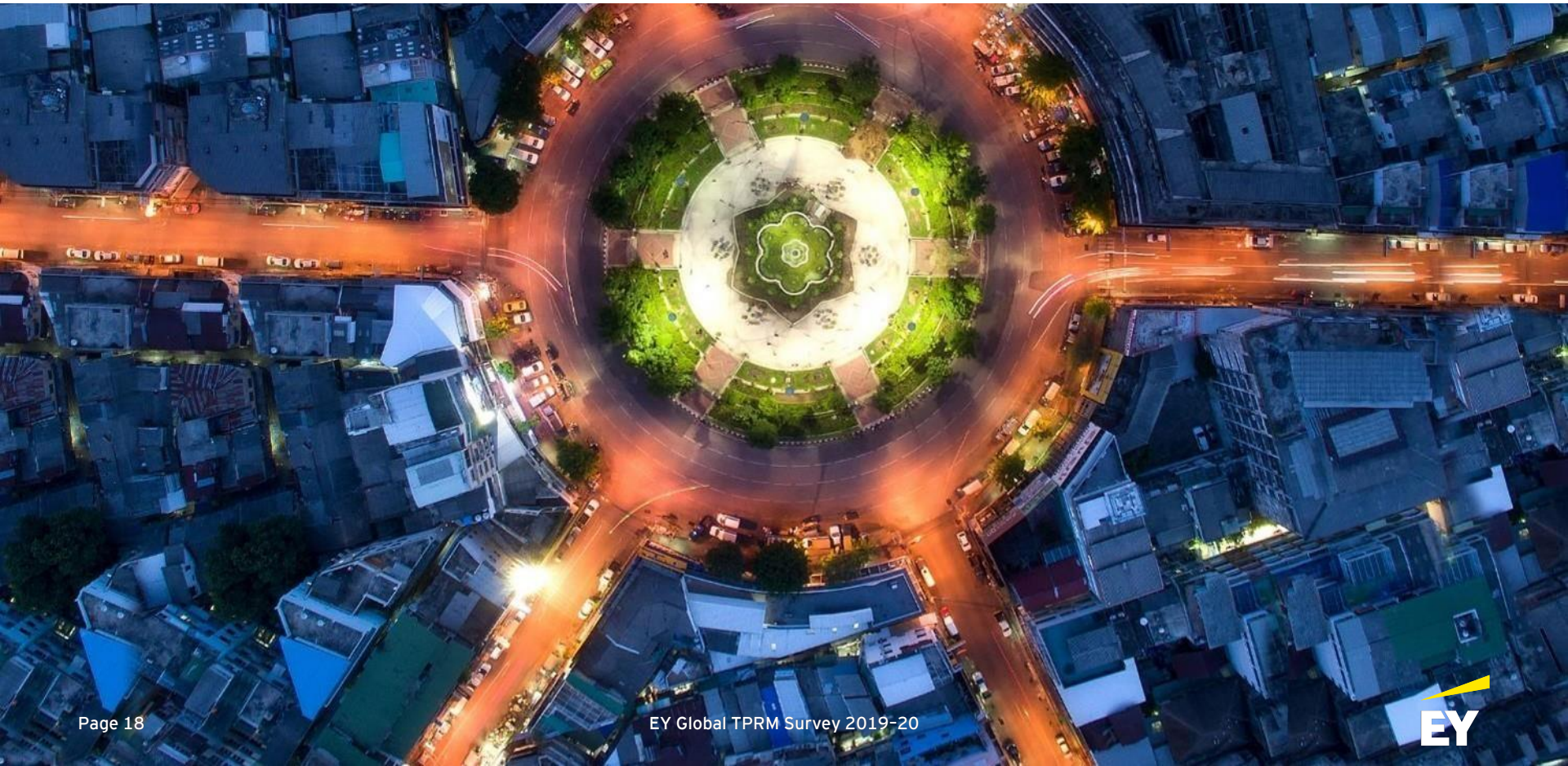


Critical third-party criteria

Q15. What are the three most important criteria your organization uses to define a critical third party?



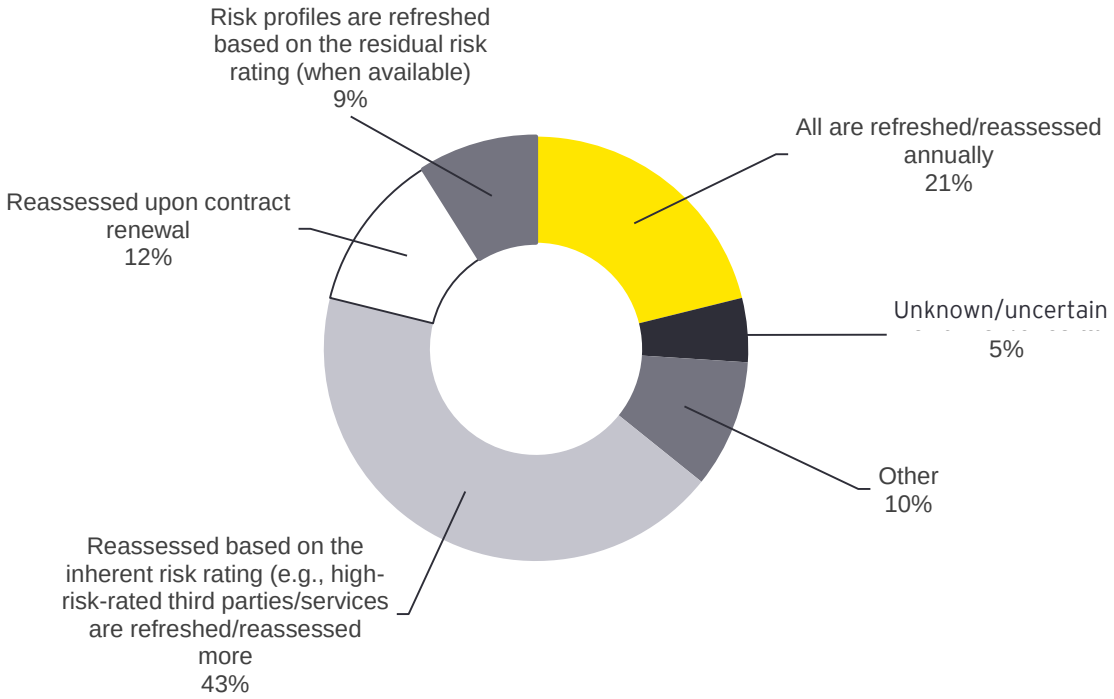
Assessments



43% of financial services organizations surveyed reassess the inherent risk profile based on the inherent risk rating while 21% reassess annually. Reassessment based on a contract event or residual risk rating are less common approaches.

Assessing inherent risk of third party

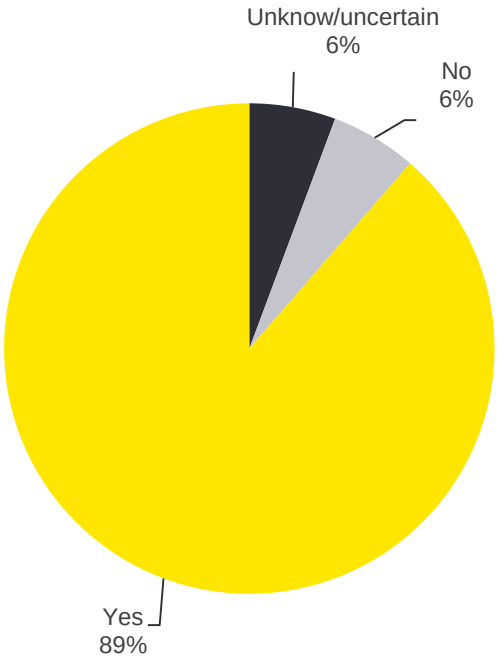
Q16. What is your organization's approach to refreshing/reassessing the inherent risk profile of your third parties?



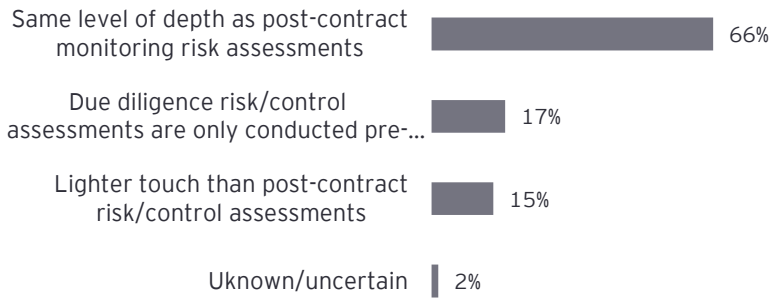
A majority of the financial services organizations surveyed (89%) conduct some form of pre-contract due diligence risk assessment. For two-thirds of the organizations, the assessments are done at the same level of depth as post-contract monitoring assessments, raising the question of whether too much is being done before a contract is signed across financial services organizations.

Pre-contract risk assessments

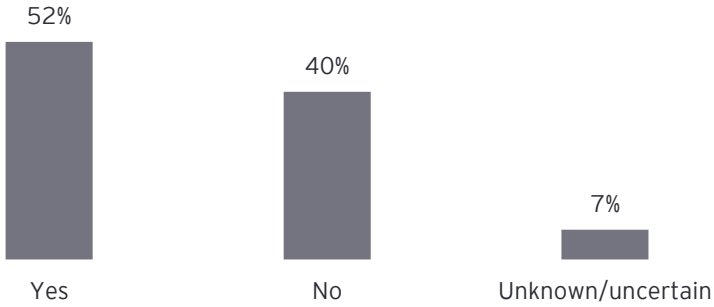
Q17. Does your organization currently conduct pre-contract due diligence risk assessments?



Q18. [If Yes to Q17] What level of depth is your organization's pre-contract due diligence risk/control assessment?



Q19. [If Yes to Q17] Does your organization have an expedited process for pre-contract risk assessments for urgent requests?



Based on financial services organizations' survey responses, the typical pre- and post-contract risk assessment questionnaires typically have between 145 and 155 questions. Cybersecurity and privacy risk account for almost half of all questions asked, aligning with respondent answers to the prior question on the most important criteria of data sensitivity (Q15).

Risk assessment questionnaire

Q20. How many questions within your organization's risk/control assessment questionnaires are used to assess third parties in each of the following risk areas?

Average number of questions

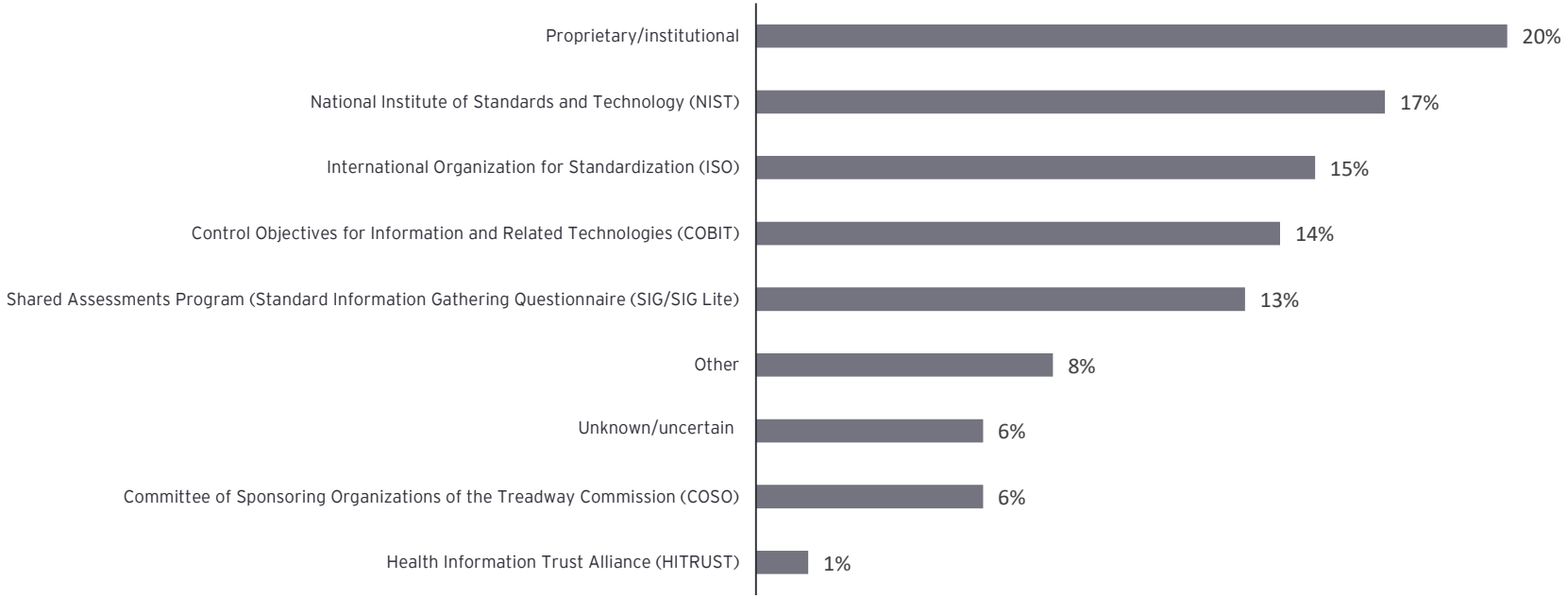
	Inherent risk assessment questionnaire	Pre-contract risk assessment questionnaire	Post-contract risk assessment questionnaire
Regulatory and compliance	6.98	24.18	27.49
Strategic risk	1.98	1.95	2.43
Cybersecurity and privacy risk	30.65	72.96	74.27
Financial risk	3.09	5.35	5.90
Business continuity and resiliency	7.97	20.16	19.55
Geopolitical risk	1.18	1.75	2.08
Digital risk	2.08	6.07	7.04
Operational risk	3.68	8.93	11.61
Brand and reputational risk	2.11	2.47	2.51
Sustainability risk	0.62	1.67	1.53
Total	60.35	145.49	154.41

Note: Average number of questions outlined are greater than 25.

One in five financial services organizations surveyed use a proprietary/institutional framework, a decrease from last year; however, there has been a significant uptick in the proportion of firms using NIST (17% of respondents). ISO (15%) and COBIT (14%) have also seen increased usage by organizations. By using industry-proven and trusted frameworks such as NIST, organizations feel comfortable with using such frameworks as a baseline.

Risk assessment questionnaire framework

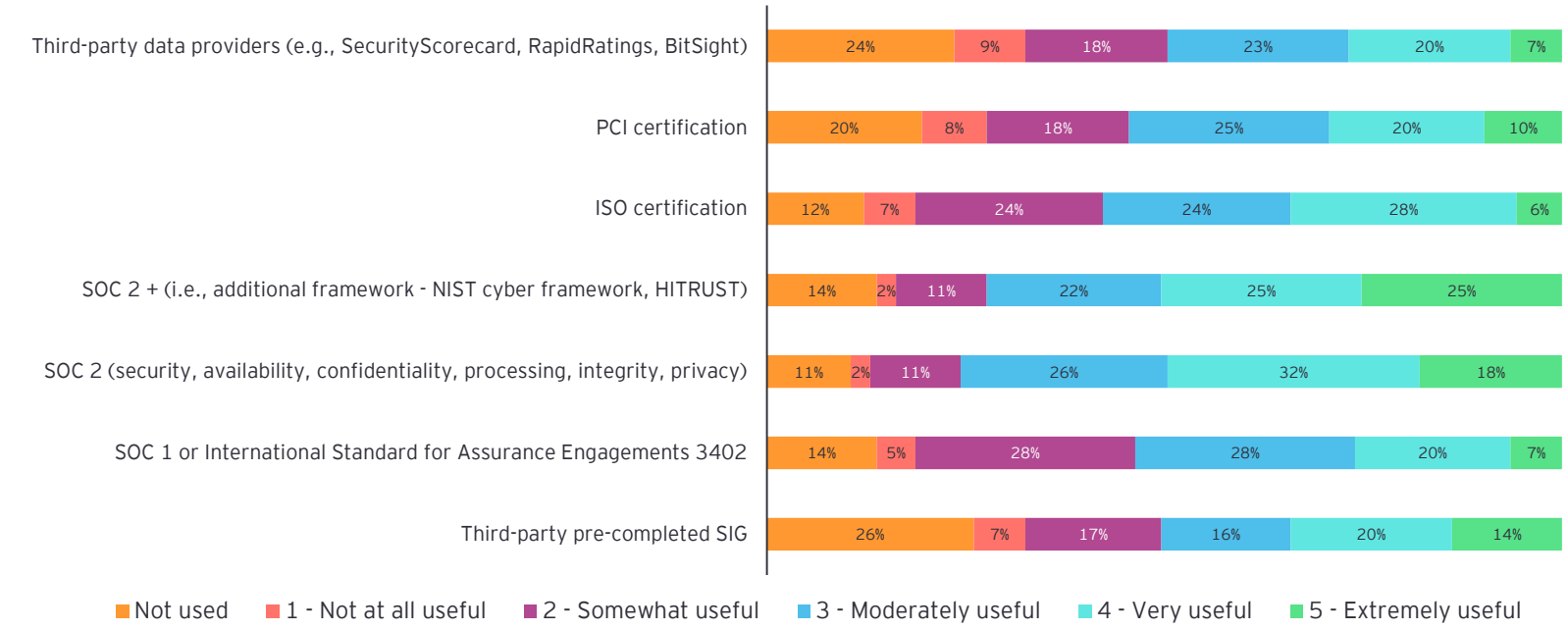
Q21. Which framework is used as a baseline for your risk assessment questionnaire?



Half of the financial services organizations surveyed found System and Organization Controls (SOC) 2 or SOC 2+ as an additional framework to be very useful or extremely useful. 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.

Usefulness of tools/documentation in reducing/removing risk

Q22. 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?



Financial services organization survey respondents indicated that reassessment is typically done every year for third parties in the highest-risk tiers while, for lower-risk third parties, reassessment is done less frequently.

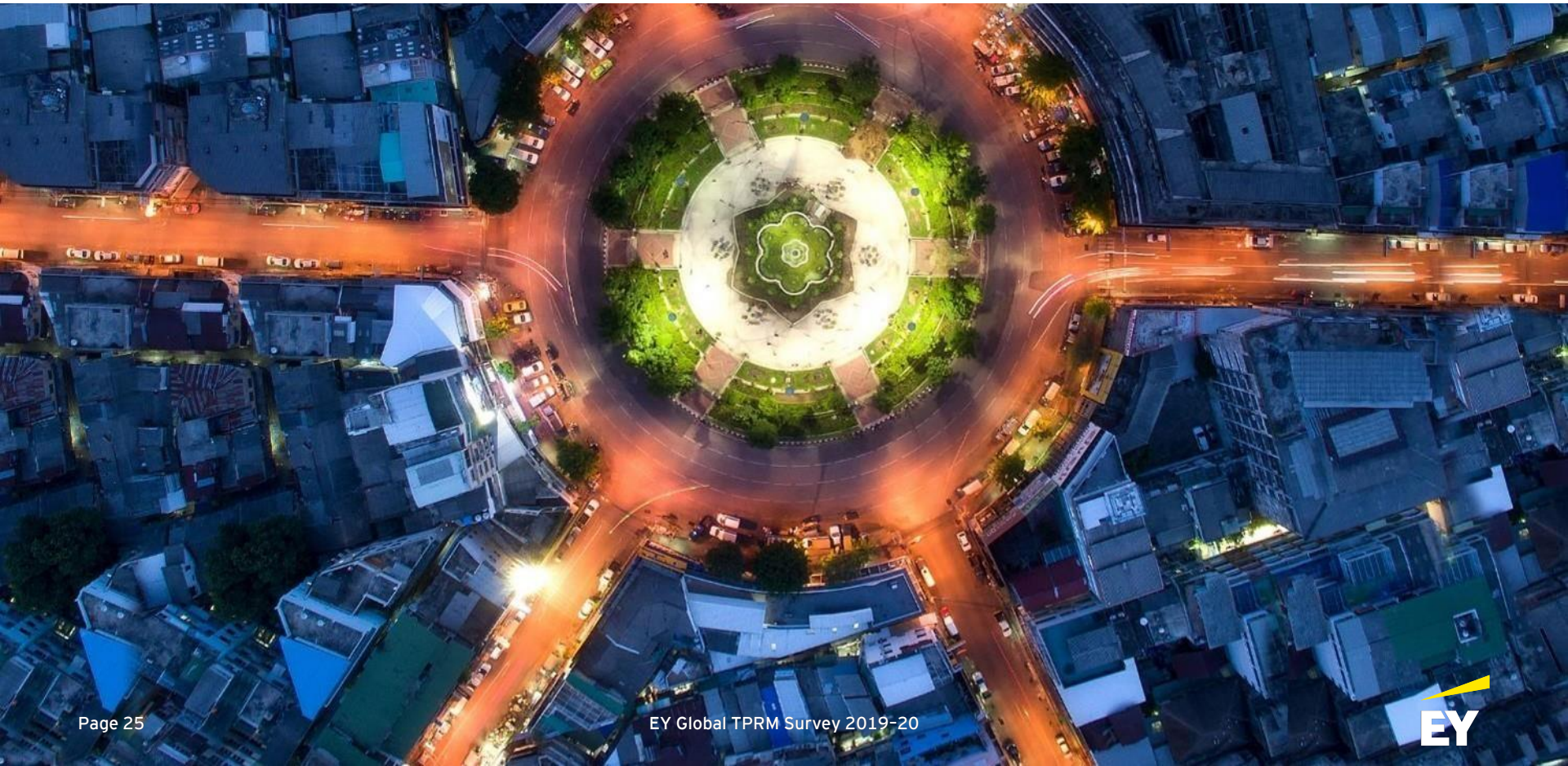
Frequency of performing third-party risk assessments

Q23. How often does your organization reassess (risk/control assessment) your third parties based on risk posed to the organization?

Risk type	Every six months	One year	Two years	Three years or more	Not assessed	Unknown/ uncertain
Critical risk	10%	**82%**	4%	1%	3%	0%
Highest risk	2%	**62%**	24%	3%	2%	6%
Second-highest risk	1%	24%	**39%**	18%	7%	11%
Third-highest risk	1%	16%	16%	**37%**	16%	13%
Remaining risk	1%	11%	7%	**30%**	**35%**	16%

Note: Outlined percentages are responses greater than 30%.

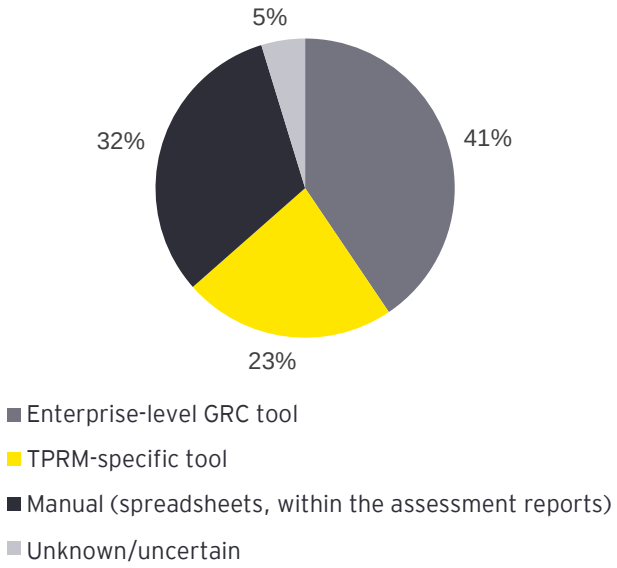
Issue management/risk treatment



Across the financial services organizations surveyed, remediation is the most common action for identified issues, with contractual changes following. Termination is more common in the critical-risk and highest-risk tiers, but still applied to third parties in the second-highest and third-highest risk tiers.

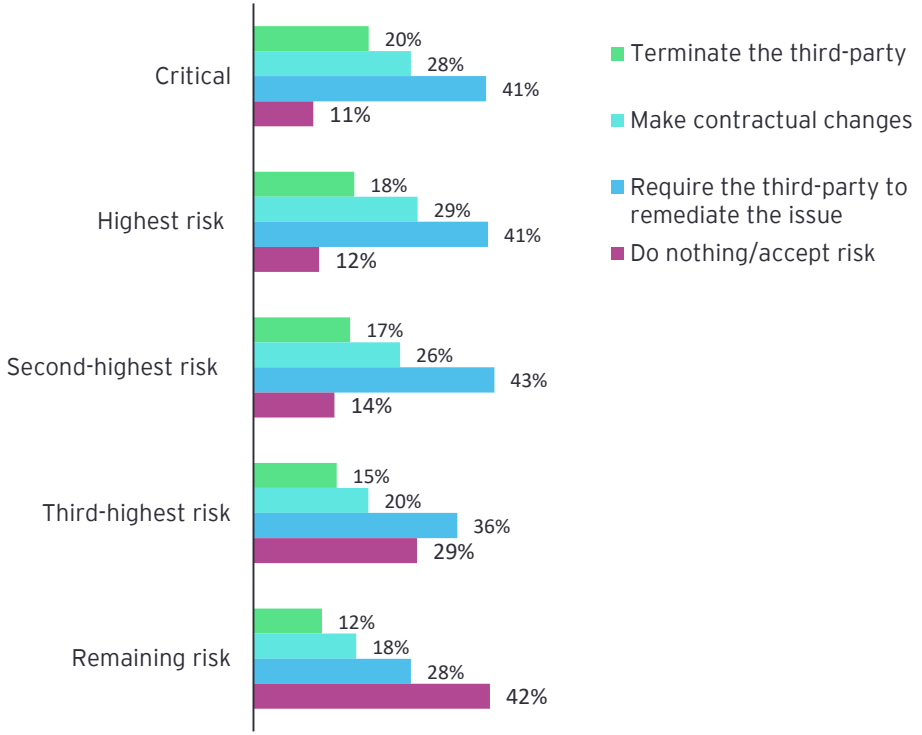
Issue tracking

Q24. How are issues and exceptions stored and tracked?



Actions for issues

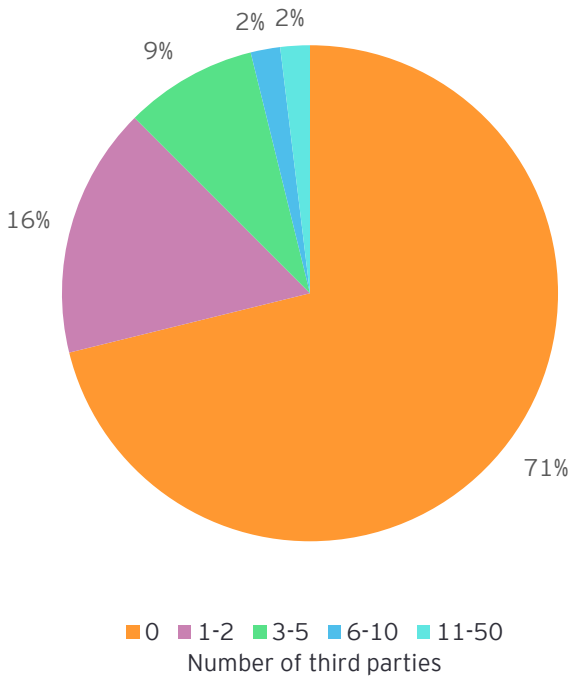
Q25. For third-party issues that you identify in each of the following risk tiers, what actions do you take?



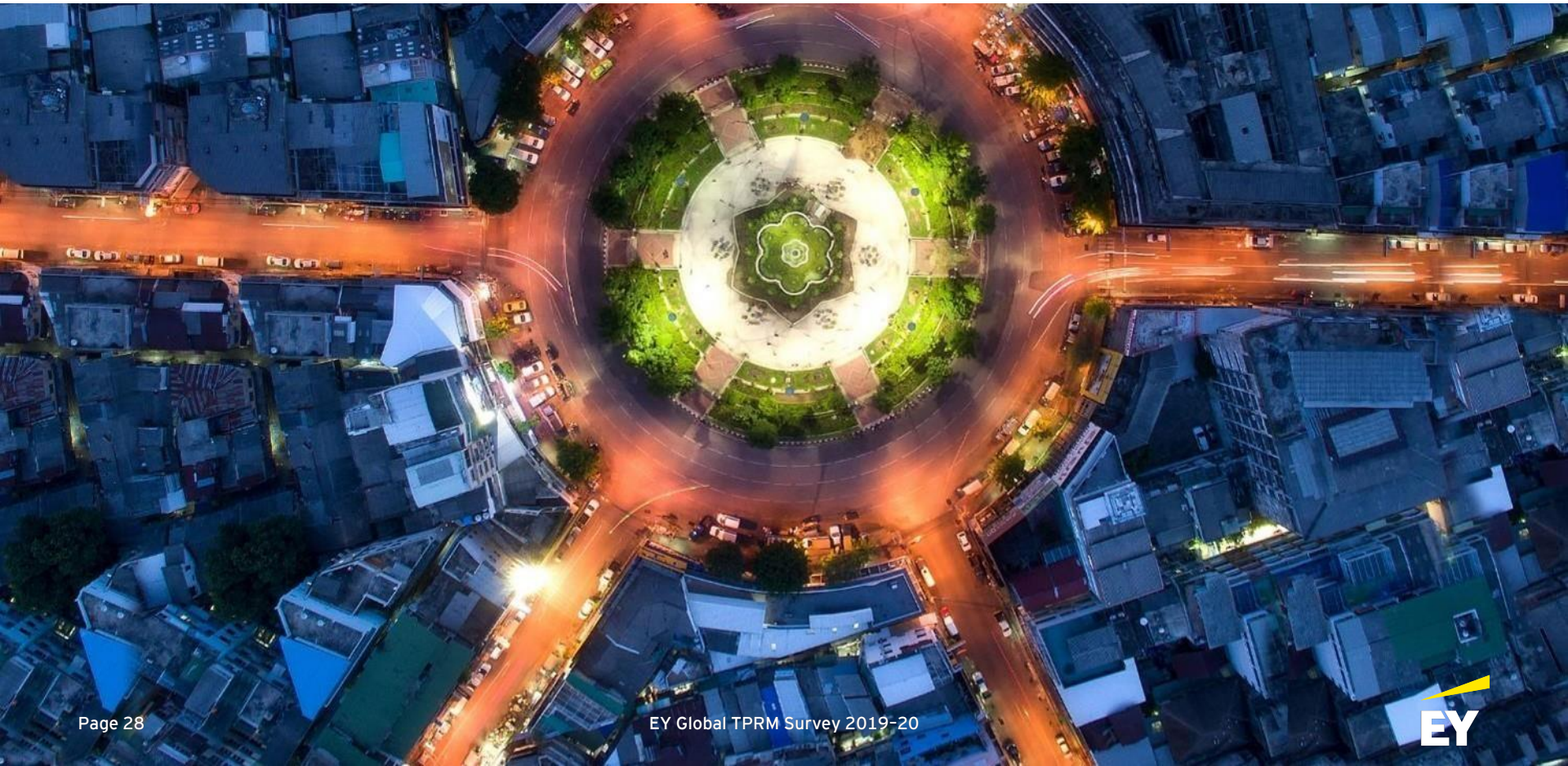
Correlating to the data on actions taken after issue identification (Q25), the most common action is remediation or contractual changes, and the majority (71%) of the organizations surveyed indicated that no third parties have been terminated due to issue identification. One-quarter of the financial services organizations terminated only one to five third parties.

Termination of third parties due to issues

Q26. Over the past 12 months, how many third parties have been terminated because of issues identified?



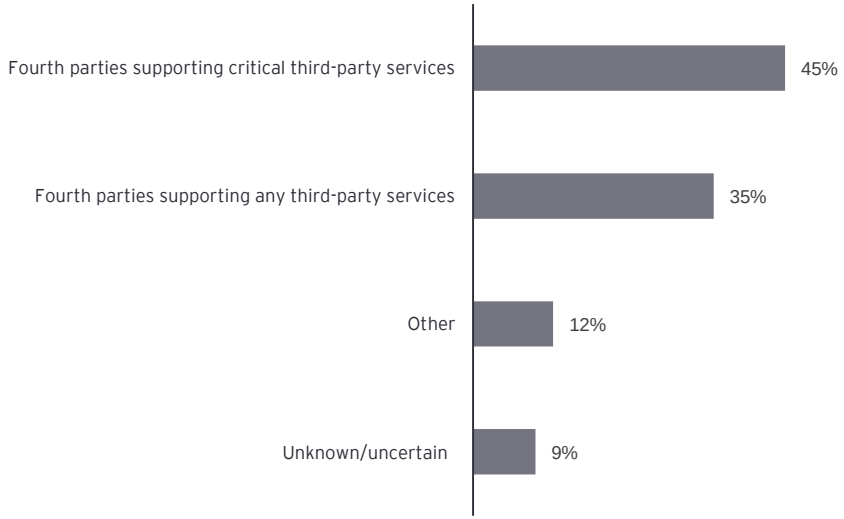
Fourth-party management



Less than half of the financial services organizations surveyed (45%) collect information on fourth parties that support critical third-party services. Only one in three of the organizations collect information on all fourth parties. Typically, fourth-party information is gathered during the risk/control assessment process. It is likely that privacy and global inventory expectations across the financial services industry will increase the collection of fourth-party data in years to come.

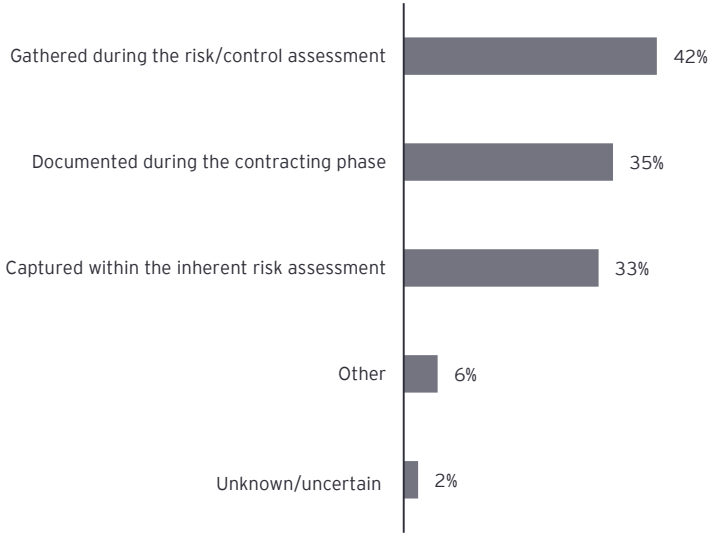
Fourth-party data collection

Q27. Which fourth parties/subcontractors does your organization collect information on?



Fourth-party data collection methods

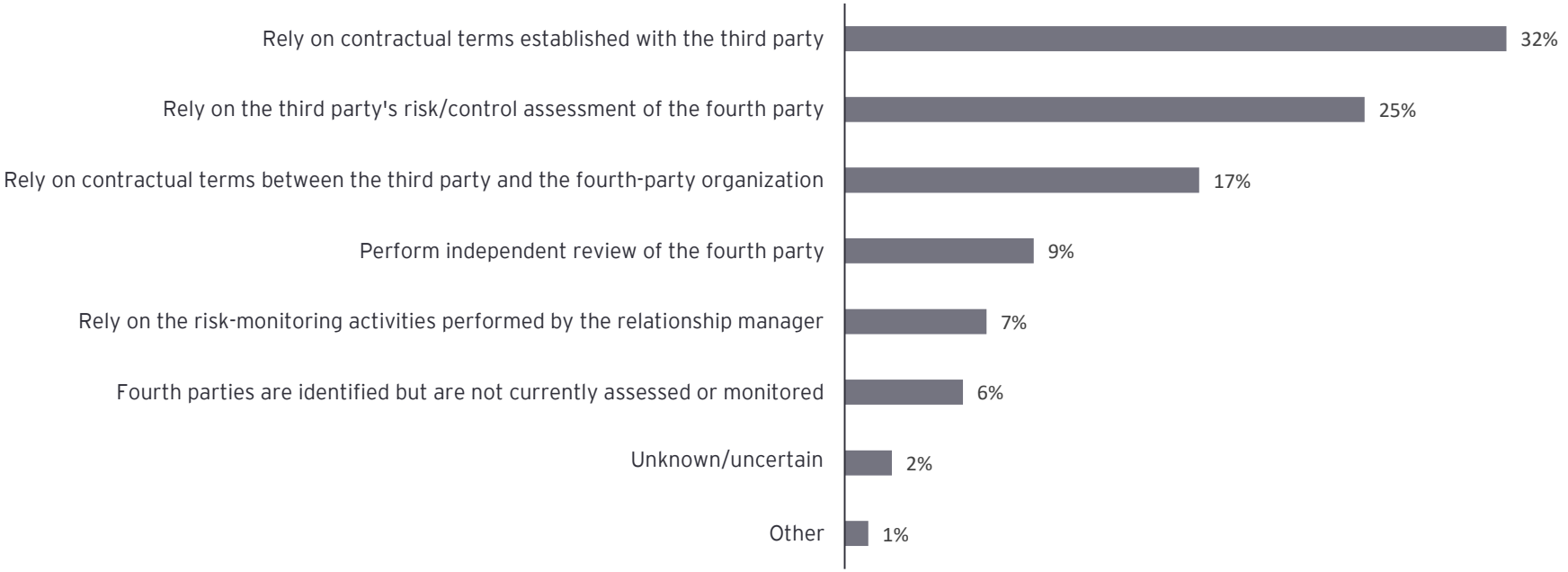
Q28. How is fourth-party information identified and collected (e.g., name, location, services provided)?



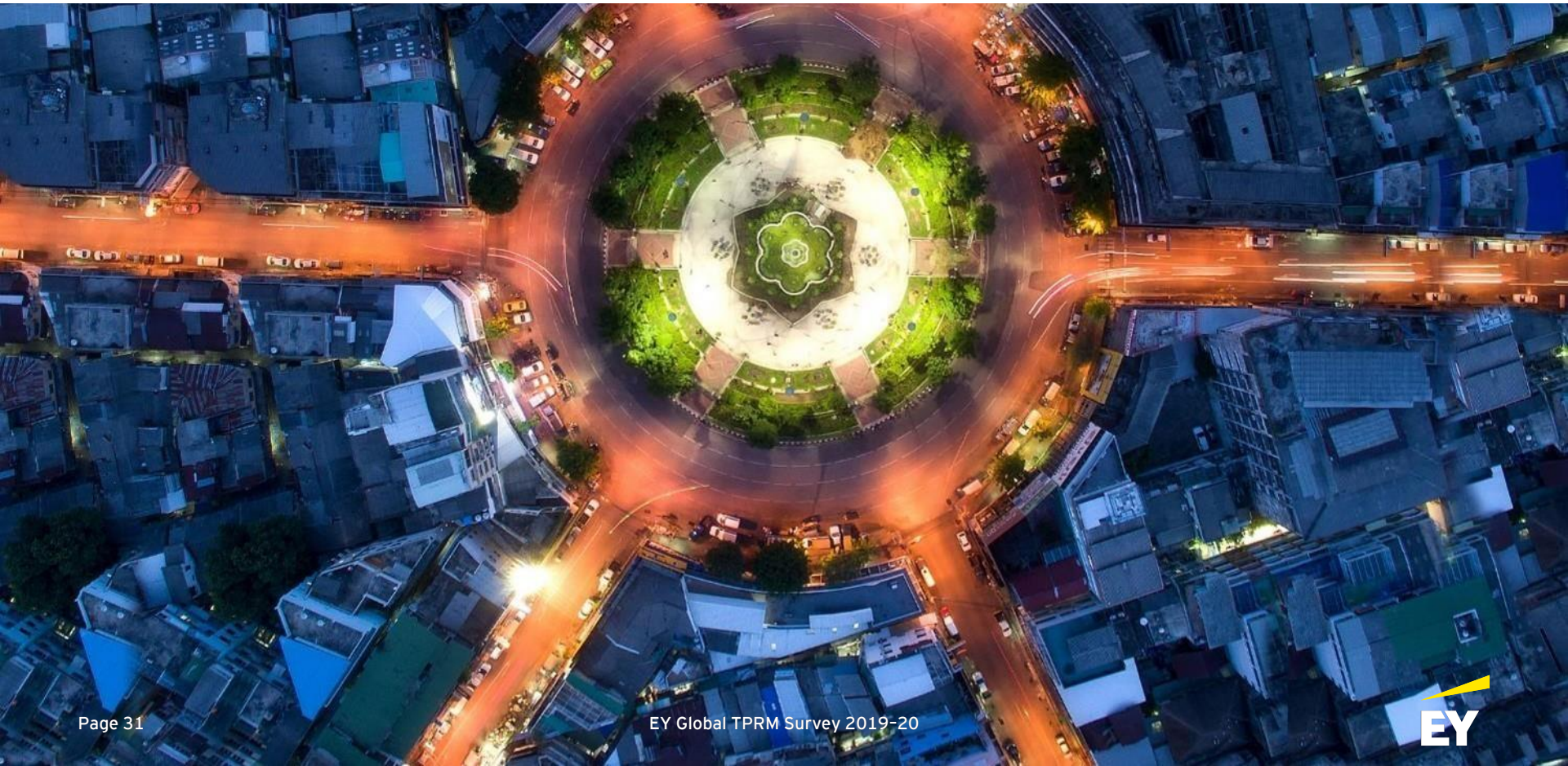
One-third of financial services organizations surveyed rely on contractual terms with their third parties for the purposes of overseeing/monitoring fourth parties. Increasingly, firms are also relying on contractual terms between the third and fourth party (25%). A minority of the surveyed organizations (9%) perform their own independent reviews of fourth parties, a figure that increased from last year but still has opportunity for improvement.

Fourth-party monitoring

Q29. How does your organization assess/monitor fourth parties?



Technology



The financial services organizations surveyed indicated that no tool or manual effort is used for approximately 20%-35% of all functions to manage risk. However, manual execution of issue management has significantly decreased, from nearly 40% last year to 21% this year, revealing that more firms are adopting technology solutions. Archer is the most common tool used, followed by SAP Ariba. Notably, respondents indicated that other tools are often used, revealing that organizations are possibly using tools from smaller or bespoke providers.

Technology tools to manage risk

Q30. What technology/tools does your organization use for each of the following functions to manage risk?

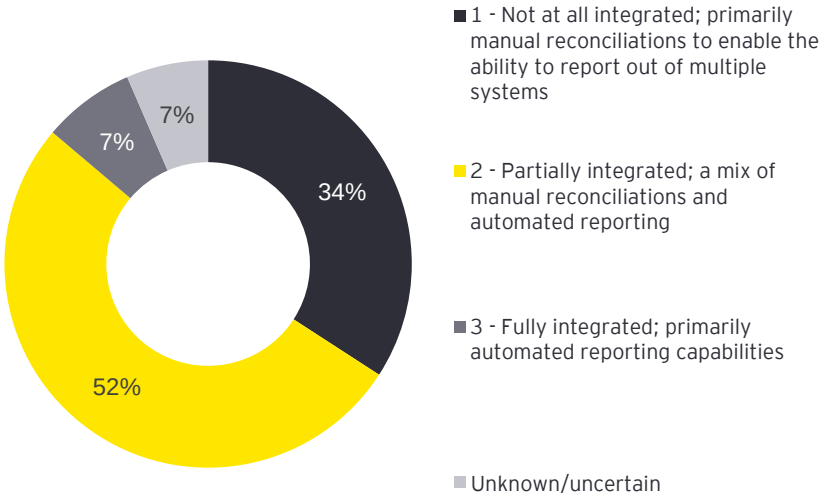
Function	No tool used (manual)	Archer®	Bwise®	Metric-Stream	SAP Ariba®	Hiperos®	Process Unity®	Prevalent®	Aravo	Service-Now	OneTrust	Lockpath	Proprietary	Other
Sourcing	35%	6%	0%	0%	29%	3%	1%	0%	0%	3%	0%	0%	6%	18%
Inherent risk assessment	23%	26%	0%	1%	3%	9%	3%	0%	3%	3%	1%	0%	18%	12%
Contract management	27%	7%	0%	0%	26%	4%	2%	0%	0%	1%	0%	0%	12%	22%
Primary third-party inventory	22%	20%	0%	1%	13%	6%	2%	0%	2%	2%	1%	0%	16%	15%
Risk/control assessment facilitation	20%	24%	2%	2%	4%	8%	4%	0%	3%	3%	2%	0%	13%	15%
Issue management	21%	29%	3%	1%	4%	4%	3%	0%	3%	6%	1%	0%	11%	17%

Note: Outlined percentages represent the top three technology/tools to manage risk per function.

Among the financial services organizations surveyed that use tools/technology as part of their TPRM programs, only 7% indicate that a technology platform is fully integrated within the organization, a slight improvement from 4% last year, but there is still vast opportunity for improvement in this area. 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, as seen in the previous question (Q30).

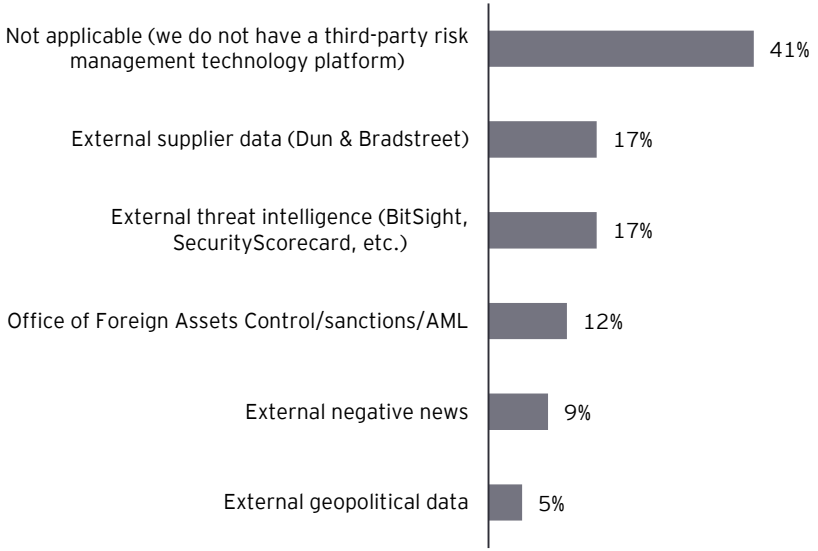
Technology integration

Q31. How well integrated are the various tools your organization uses as part of your third-party risk management program/function?

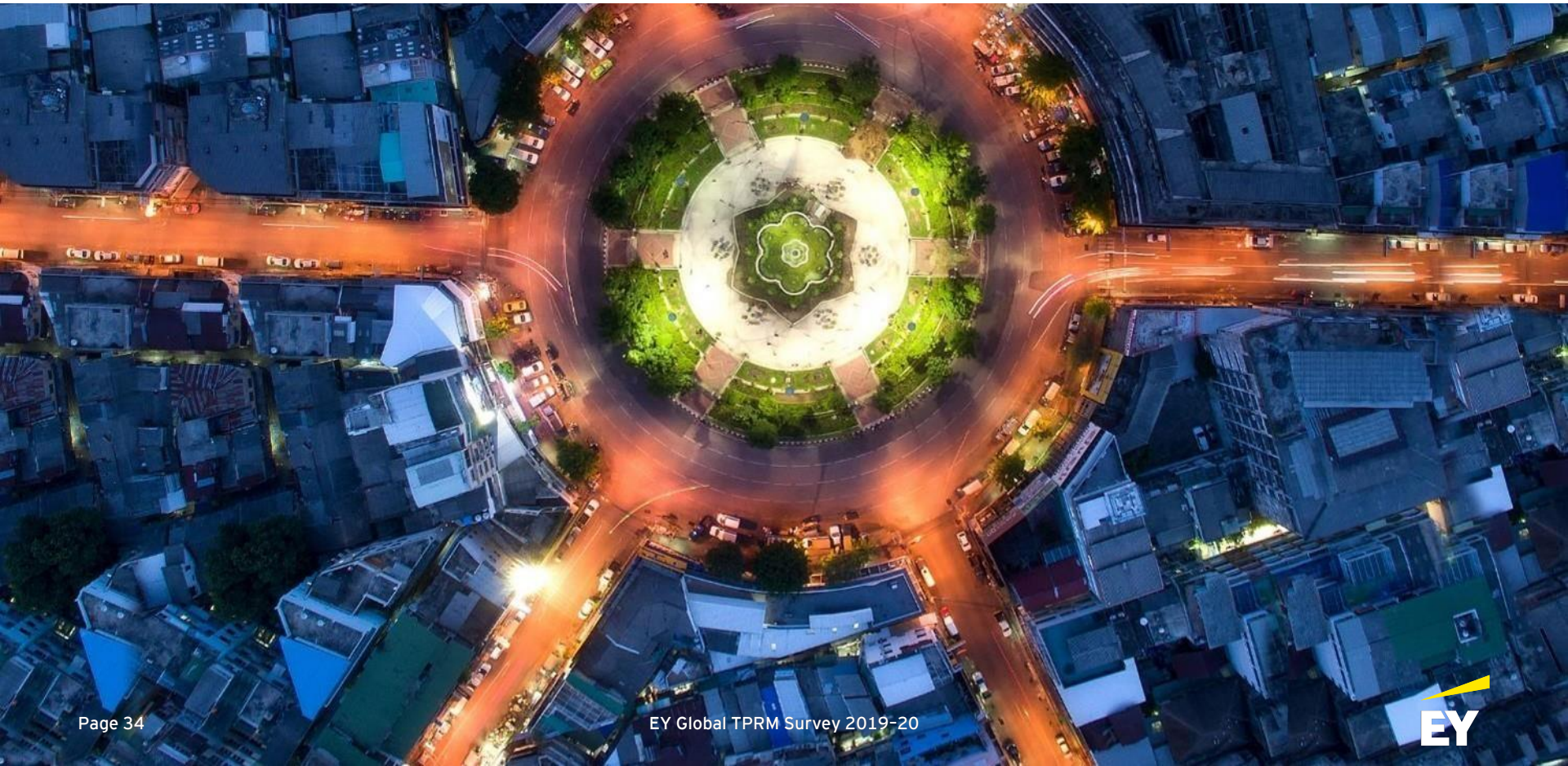


Technology integration

Q32. 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?



Reporting



The number of surveyed financial services organizations that report to the board about the TPRM program is still low. Typically, senior management is the highest level within the organization that receives regular reporting on most aspects of the TPRM program. When it comes to critical third parties, two-thirds of the organizations surveyed report on them to senior management, a 6% increase from last year.

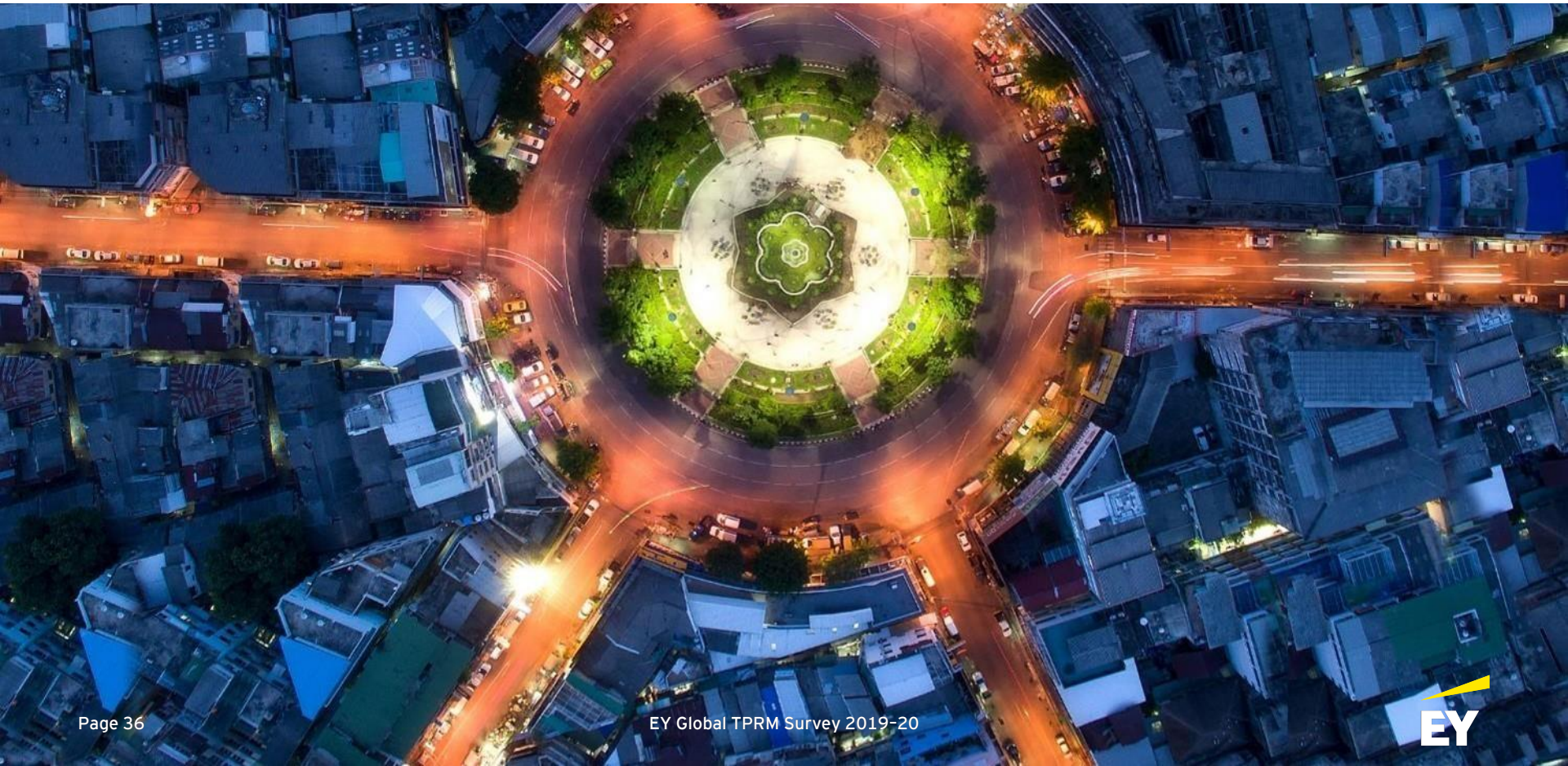
Reporting for TPRM

Q33. Which groups receive reporting for each of the following components of your third-party risk management program/function listed below?

TPRM component	Board of directors	Senior management	Business management	Third-party relationship manager	No reporting
Operational metrics of the program	31%	55%	53%	41%	13%
KPIs/KRIs	28%	58%	50%	36%	11%
Third-party landscape	30%	54%	40%	28%	11%
Critical third parties	41%	66%	54%	38%	7%
Third parties with breaches or incidents	37%	69%	63%	49%	4%
Third parties with significant issues	32%	65%	63%	49%	6%
Third parties terminated prior to contract end date	9%	34%	44%	36%	18%

Note: Outlined percentages are greater than 60%.

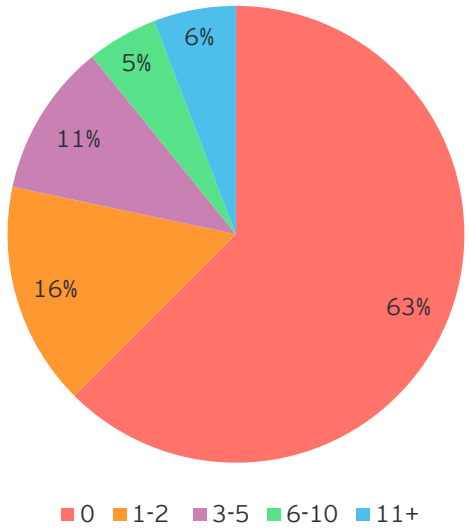
Cybersecurity and threat intelligence



Similar to last year's results, a significant number of the financial services organizations surveyed have faced breaches or outages caused by third parties. Over one in five organizations reported having at least three breaches, while over one in three reported at least three outages.

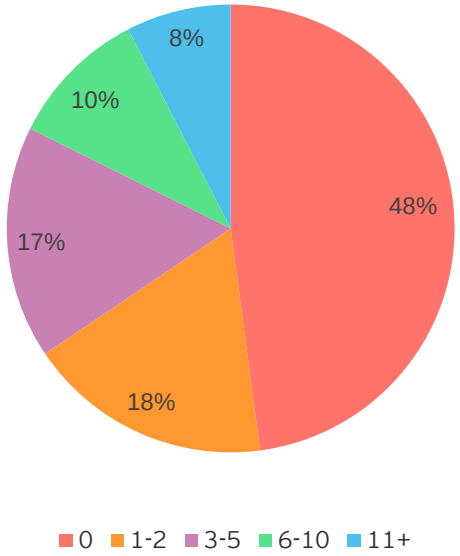
Data breaches caused by third parties

Q34. Over the past two years, how many data breaches or losses have been caused by third parties?



Outages caused by third parties

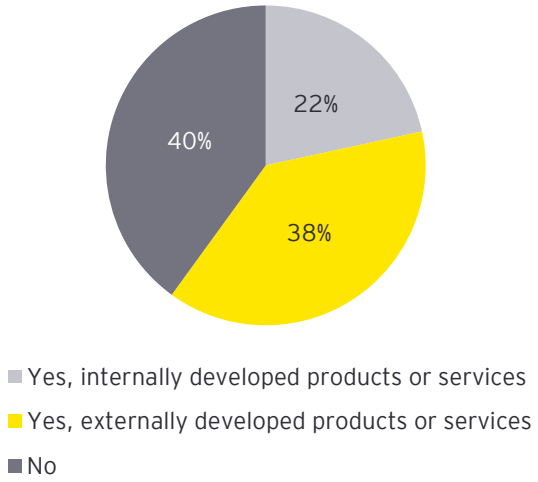
Q35. Over the past two years, how many outages have been caused by third parties?



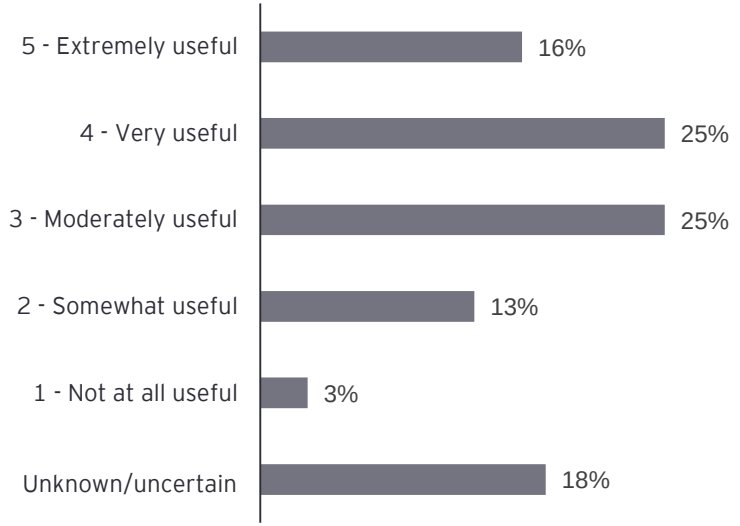
Despite the significant number of financial services organizations surveyed that have suffered a breach, nearly half of them do not utilize threat intelligence tools. This may be driven by the fact that only 41% found threat intelligence tools to be extremely or very useful at driving risk-based ongoing oversight activity.

Threat intelligence

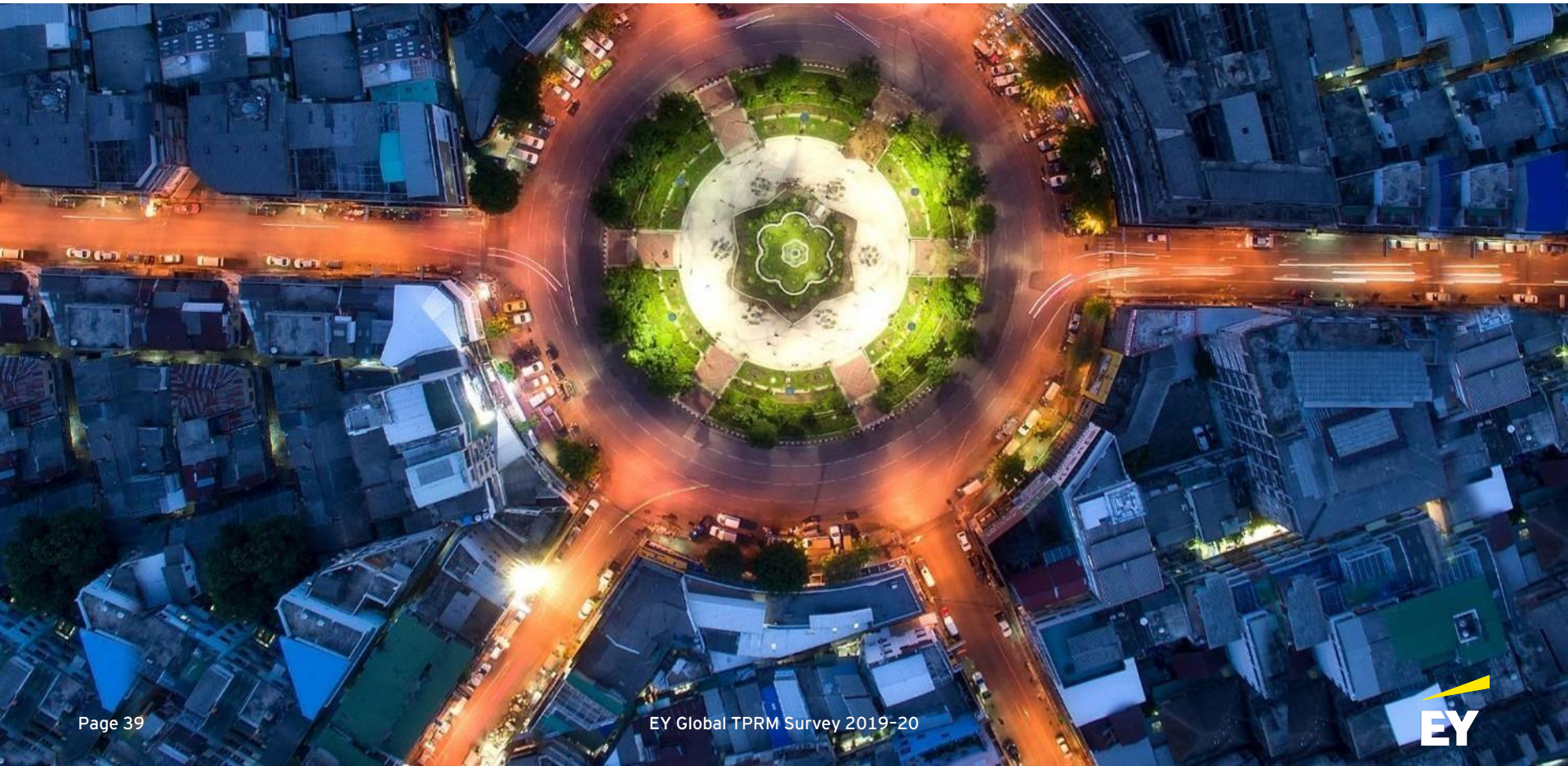
Q36. Does your organization utilize threat intelligence products or services to continuously monitor the cybersecurity environment of your third-party providers?



Q37. [For those who answered Yes] On a scale of 1 to 5, with 1 being not at all useful and 5 being extremely useful, how useful are threat intelligence tools at driving risk-based ongoing oversight activity?



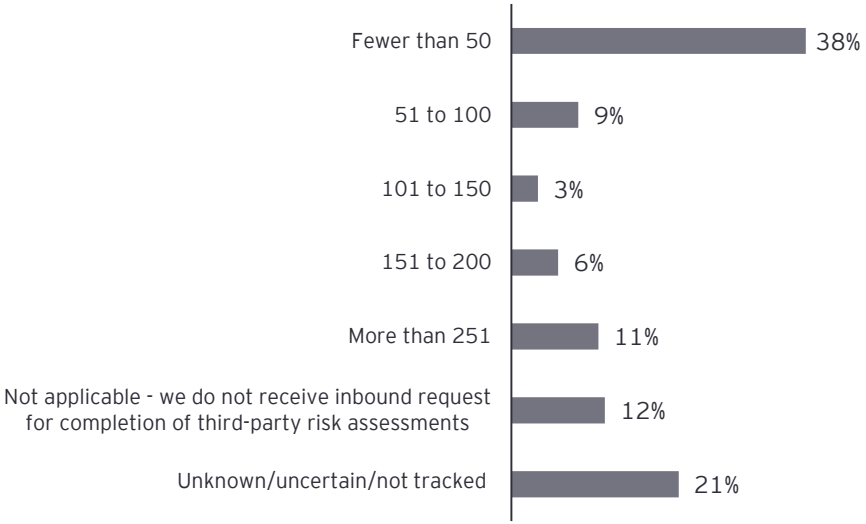
Inbound requests



Twenty-nine percent of the financial services organizations surveyed facilitate more than 50 inbound assessments per year, and an additional 21% of participants don't even know if they are being assessed, The percentage of on-site vs. remote assessments varies significantly depending on third-party volume (Q12); for organizations with more than 500 third parties assessed, the percentages shift to 8% remote and 92% on-site. That figure changes to 3% remote and 97% on-site for organizations that assess more than 1,000 third parties.

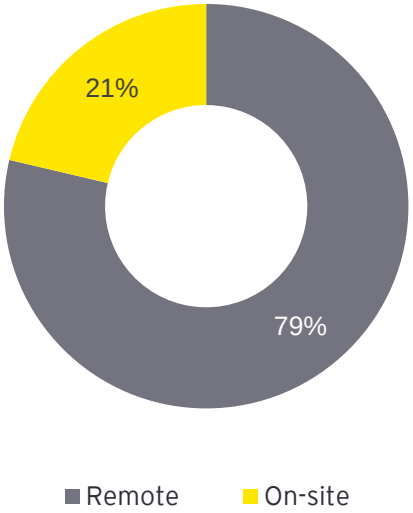
Inbound requests for TPRM

Q38. Approximately how many inbound requests for completion of third-party risk assessment questionnaires does your organization receive annually?



On-site vs. remote reviews

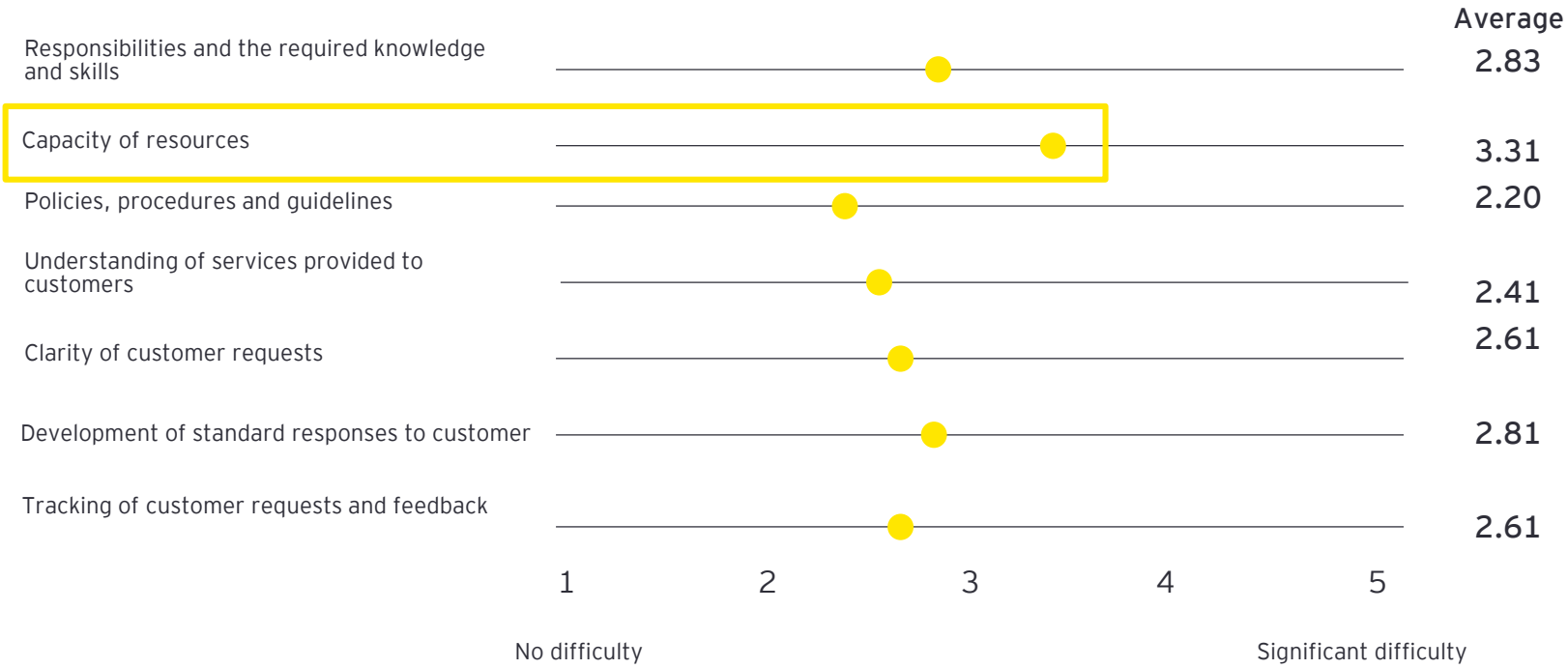
Q39. What percentage of inbound requests are on-site third-party reviews vs. remote reviews? Please provide percentages for each; total must equal 100%.



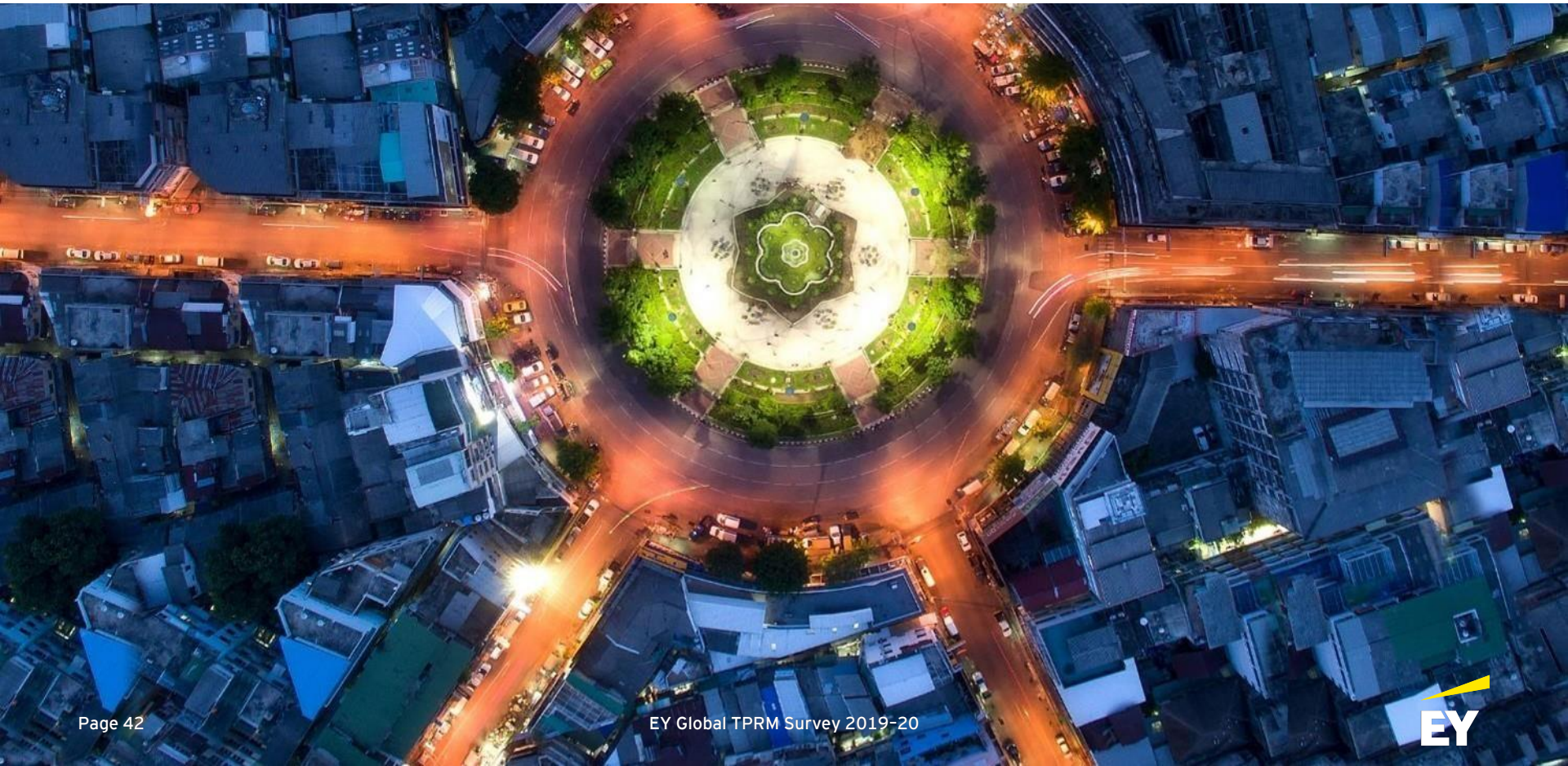
When it comes to inbound requests, capacity of resources is the most difficult challenge, followed by responsibilities and the required knowledge and skills. This is in alignment with organizations indicating that they plan to use more internal resources for TPRM execution in the next two to three years (Q7).

Difficulty related to inbound TPRM

Q40. On a 5-point scale, with 1 representing no difficulty and 5 representing significant difficulty, what degree of difficulty does your organization face in addressing each of the following related to inbound third-party risk management?



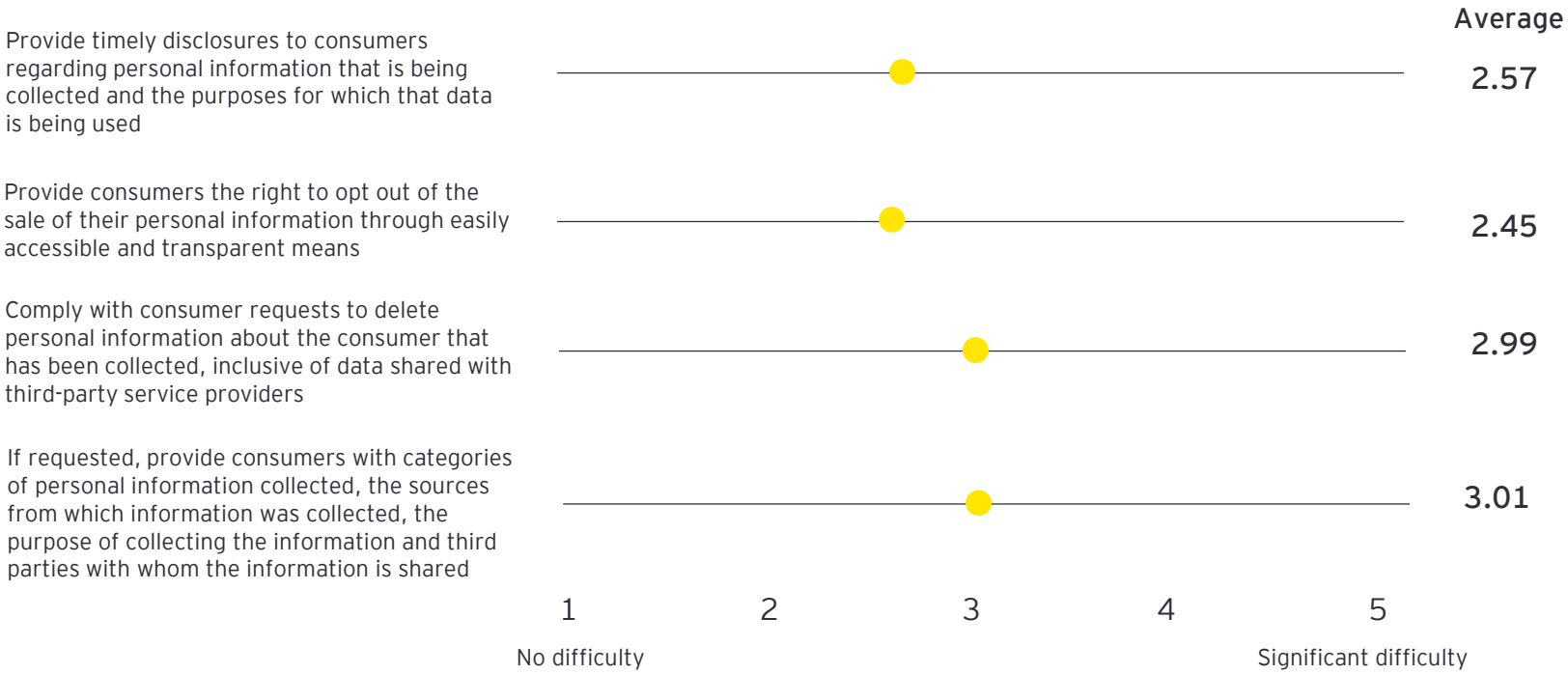
Privacy regulations



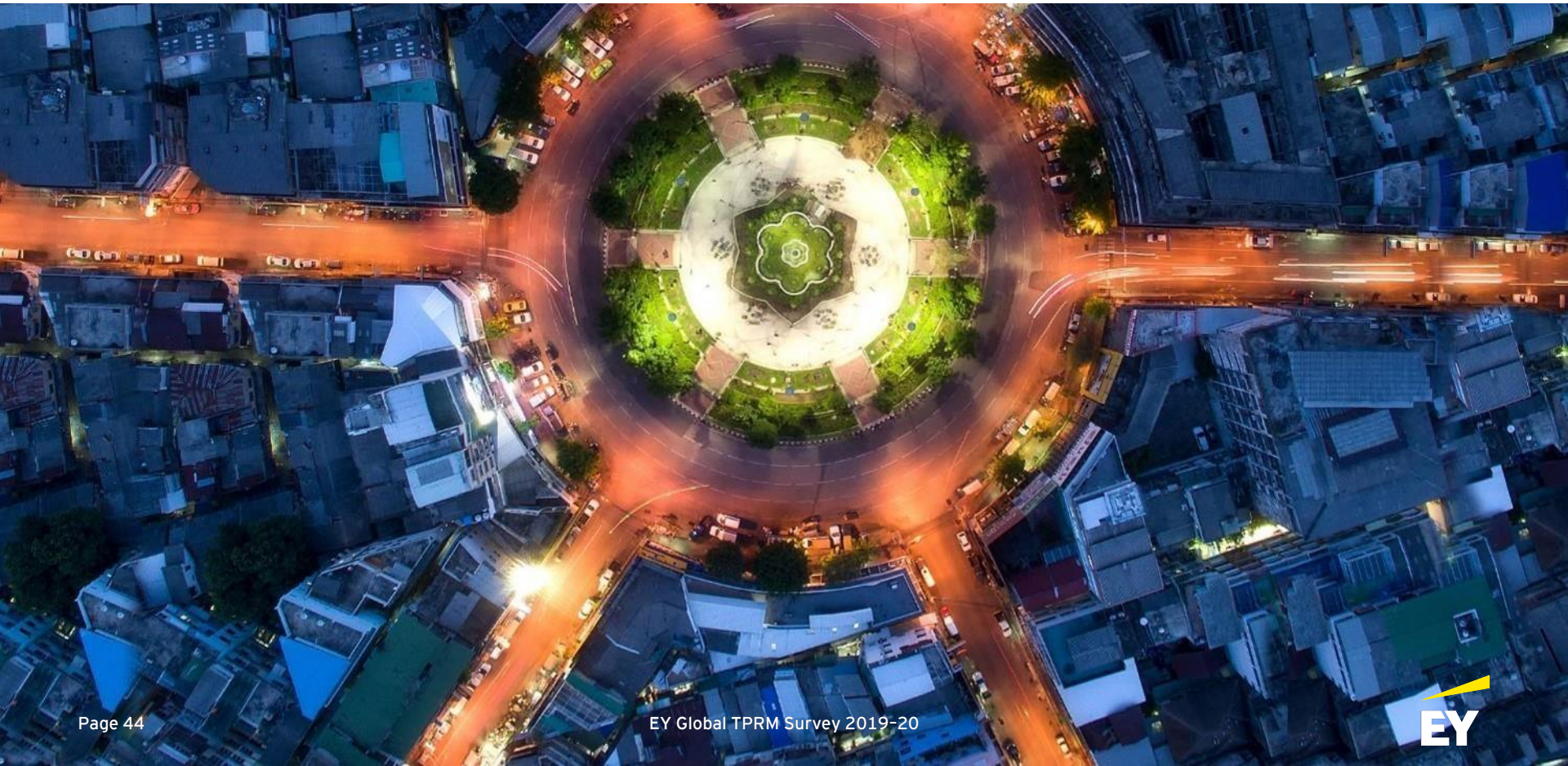
Financial services organizations are not yet fully prepared to address all aspects of recent privacy regulations (CCPA, GDPR, etc.). In particular, the organizations surveyed feel it will prove challenging to provide customers the right to opt out of the sale of their personal information and offer timely disclosures regarding the information that they are collecting and how it will be used.

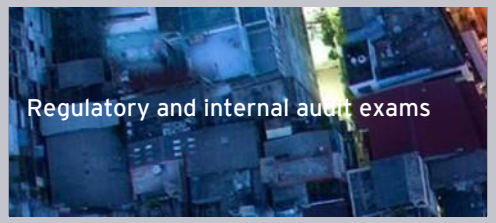
Privacy regulations in TPRM

Q41. On a scale of 1–5, how difficult will it be to address the expectations of the guidance specific to the privacy laws (e.g., GDPR, CCPA) as they relate to your third-party population?



Regulatory and internal audit exams





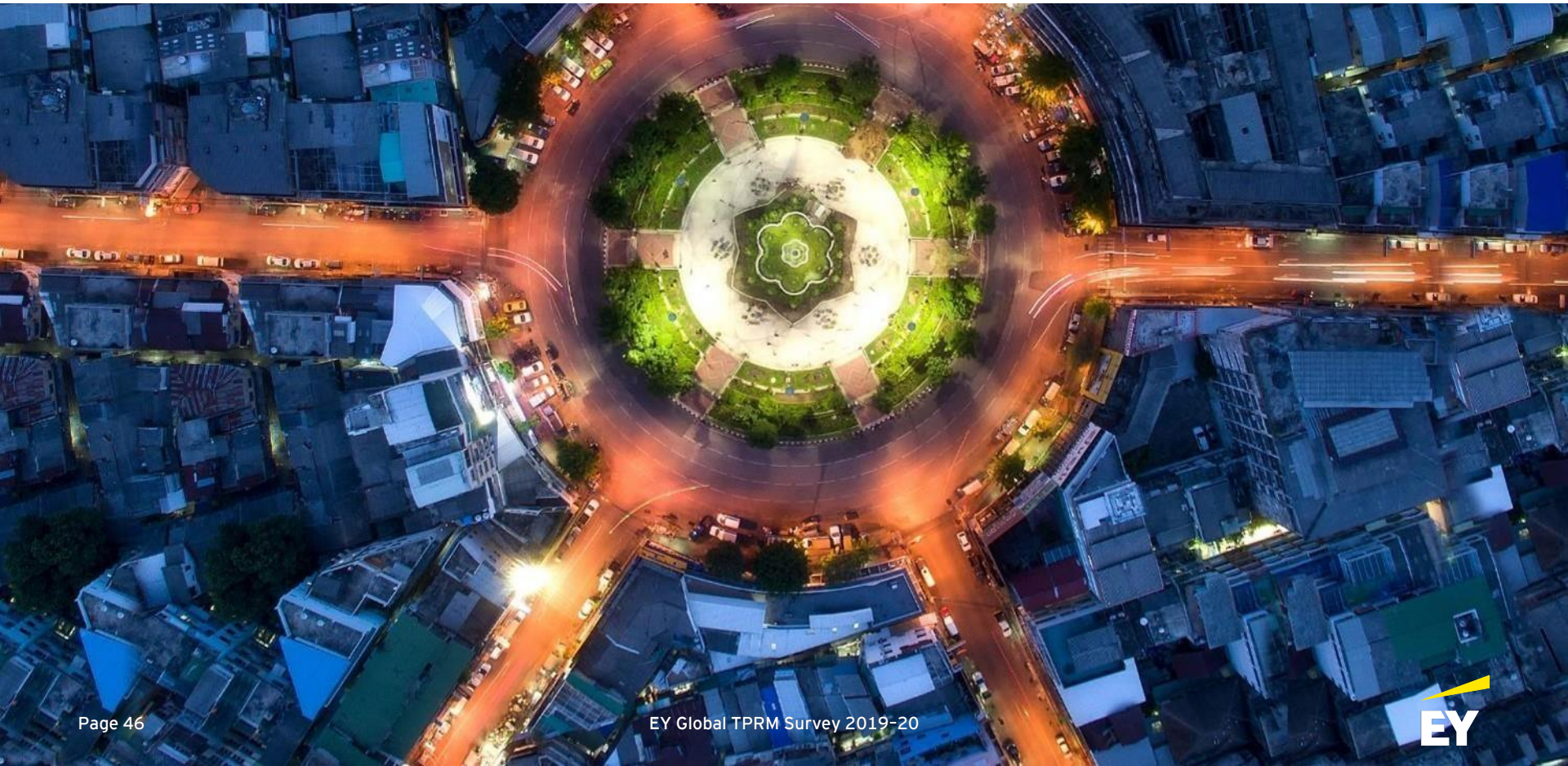
Similar to last year, oversight and governance and cybersecurity were the dominant areas of focus among the financial services organizations surveyed for regulatory body review and internal audit. In general, there is a gap there was a gap in focus between the reviews executed by internal audit and regulatory review.

Areas of focus during regulatory body review and internal audit

Q42. During your organization's most recent regulatory body review 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.

Important areas of focus	Regulatory body review	Internal audit
Oversight and governance	52	59
Cybersecurity	28	21
Enterprise-critical third parties	23	16
Third-party assessments – information security and business continuity	19	18
Fourth-party oversight and governance	14	5
Inherent risk assessment	12	19
Operating models	11	14
Privacy/confidentiality	9	9
Third-party assessments – compliance	8	12
Issue management and/or risk acceptance	7	16
Maintenance of third-party inventory	6	16
Onboarding activities	5	22
Non-traditional third parties (i.e., brokers, agents, financial intermediaries)	5	2
Foreign-based third parties	3	3
Residual risk model	2	3
Consumer protection/compliance	2	2
Other	2	3
Third-party assessments – performance	1	6
Not applicable	20	17

Non-traditional third parties



Of the financial services organizations surveyed, the most likely non-traditional third parties to be covered by TPRM are strategic partnerships, law firms providing outside legal counsel and insurance carriers. The most likely not to be covered by TPRM are charitable organizations and sponsorship partner.

Non-traditional third parties

Q43. For each of the following types of non-traditional third parties, are the third parties covered by your third-party risk management program/function?

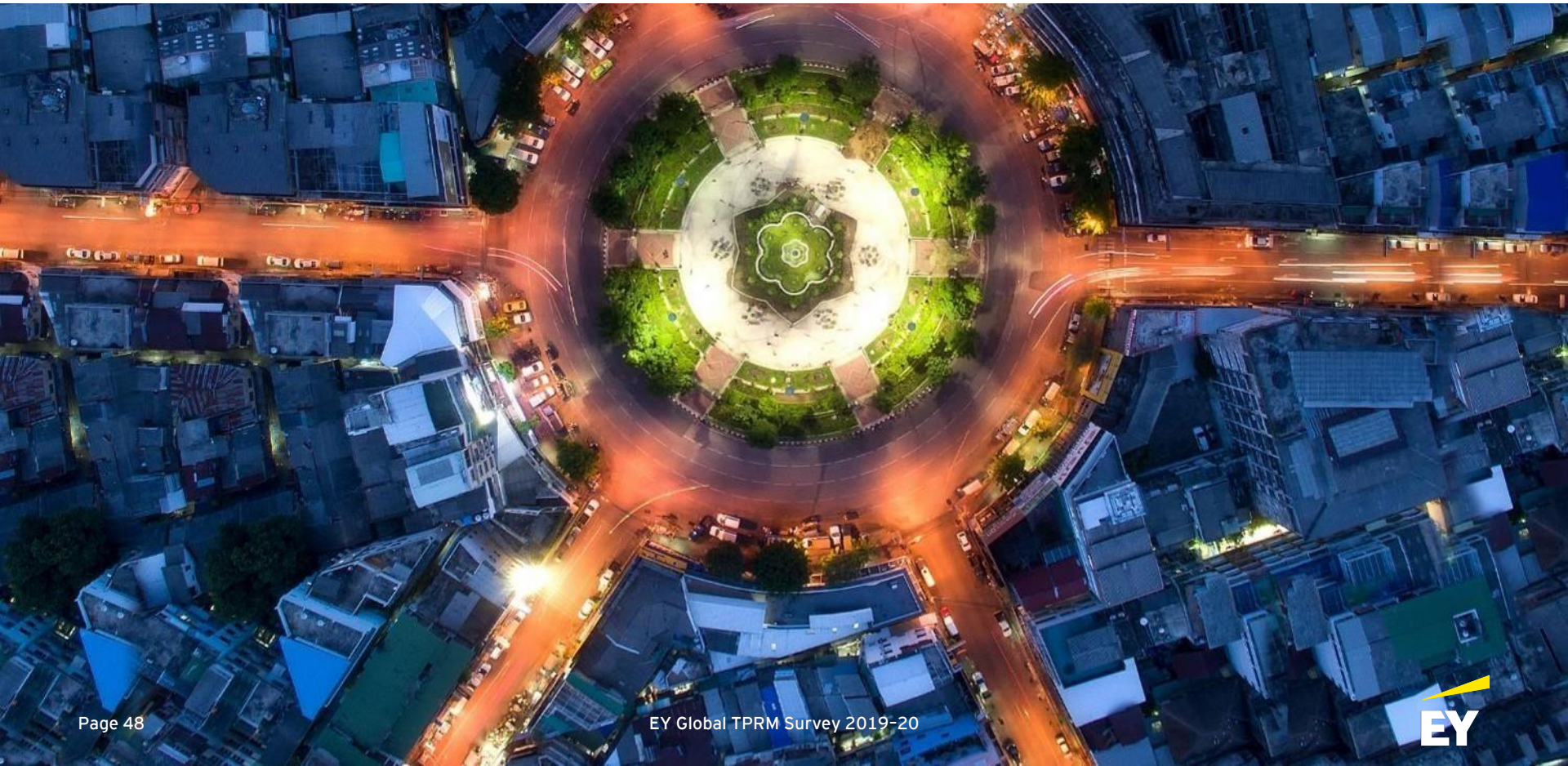
Non-traditional third parties*

Strategic partnerships	Law firms providing outside legal counsel (litigation)	Insurance carriers	Broker-dealers
34% / 55% / 11%	27% / 55% / 18%	28% / 52% / 20%	34% / 41% / 24%
Correspondent banks (agent banks)	**Financial market infrastructures**	**Joint ventures**	**Landlord's premises**
34% / 42% / 24%	32% / 48% / 19%	40% / 44% / 16%	49% / 29% / 22%

Covered by TPRM | Covered by specialized program | Not covered

* Results shown for the most common non-traditional third parties based on survey results.

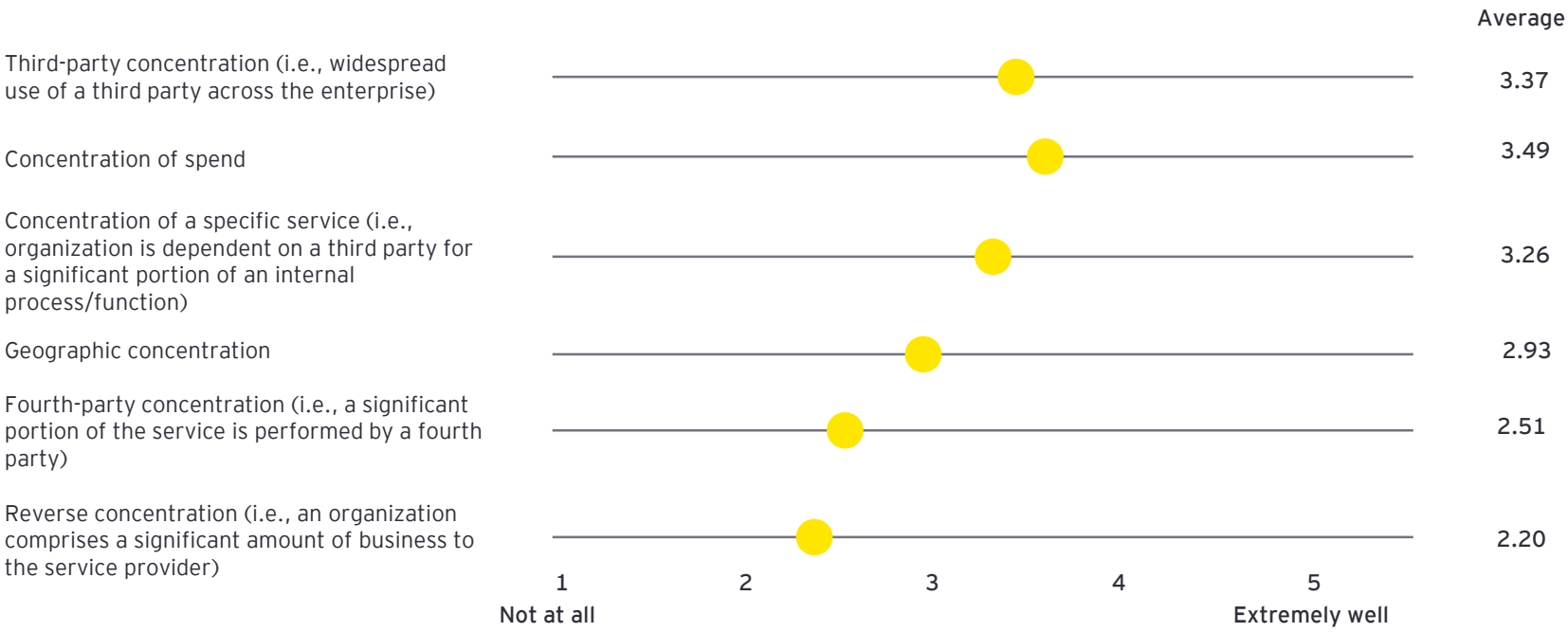
Concentration risks



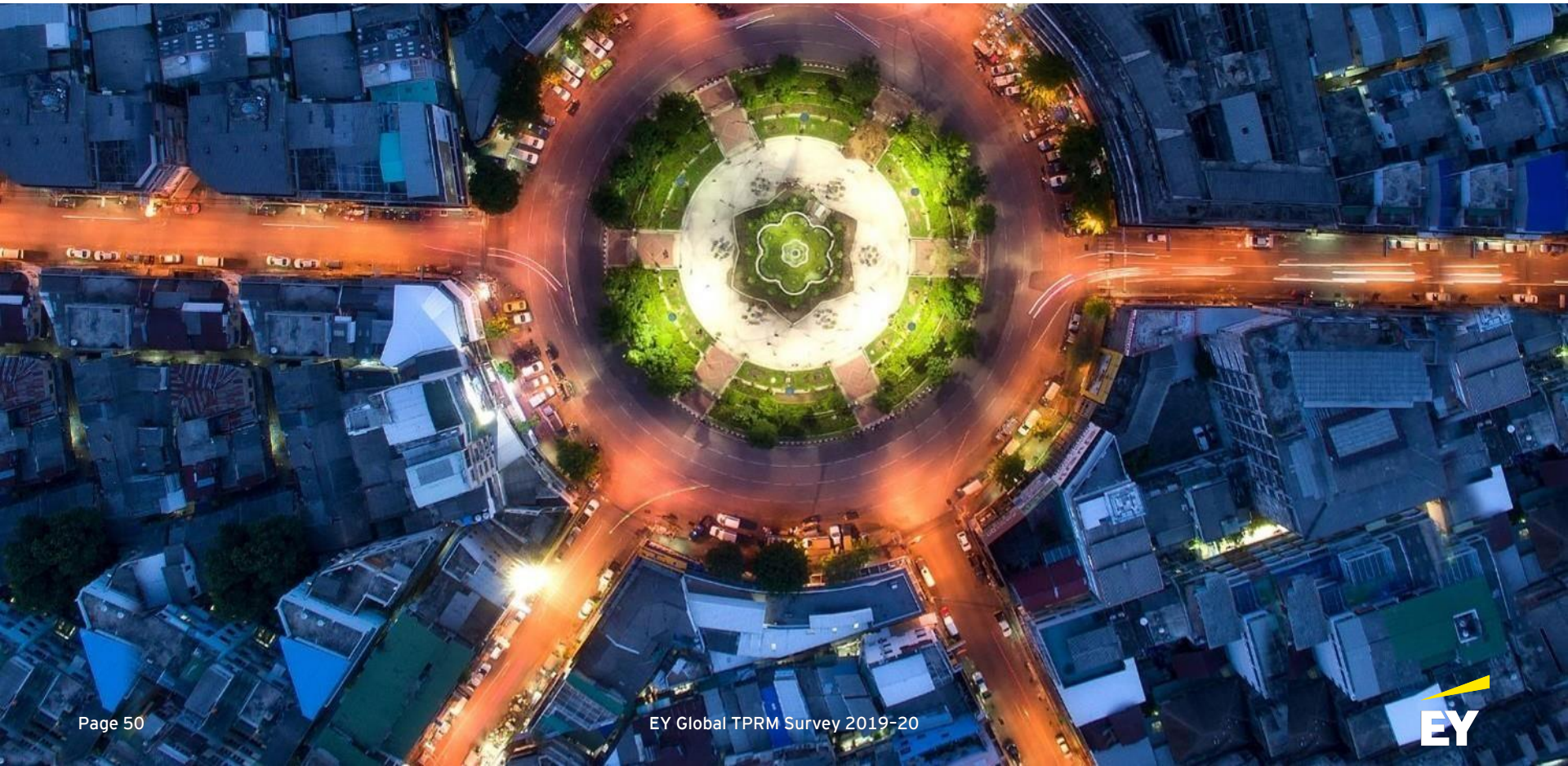
About half of the financial services organizations surveyed find it relatively easy to report on concentration of spend and third-party concentration, but far fewer find it easy to report on fourth-party or reverse concentration.

Financial services concentration risk

Q45. On a scale of 1–5, what is your organization's ability to report on each type of concentration risk, with 1 being not at all and 5 being extremely well?



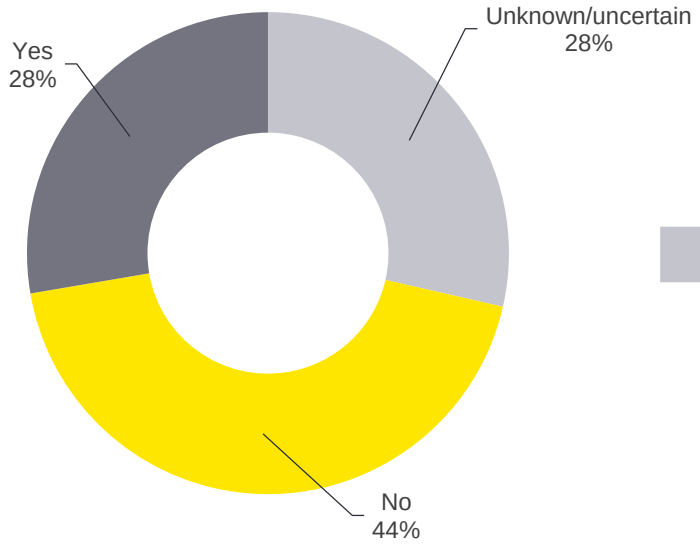
Affiliate management



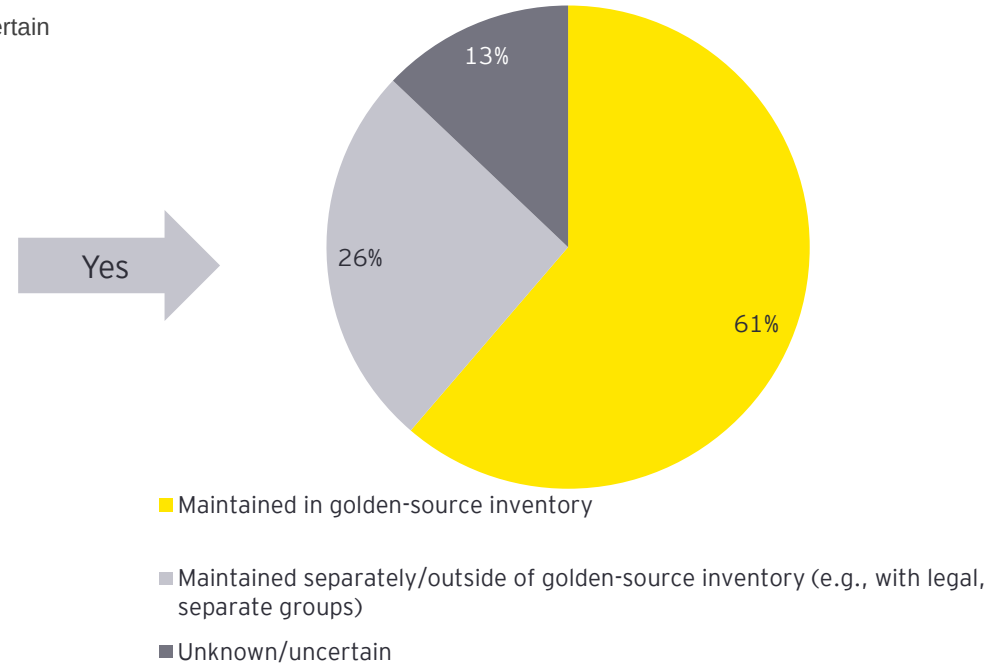
Twenty-eight percent of the financial services organizations surveyed have intercompany affiliates that are in-scope for their TPRM programs. Of those, 61% maintain those intercompany affiliates as part of their golden-source inventory.

Intercompany affiliates providing goods/services for TPRM

Q46. Are intercompany affiliates providing goods/services to your organization's US operating unit in scope for third-party risk management?



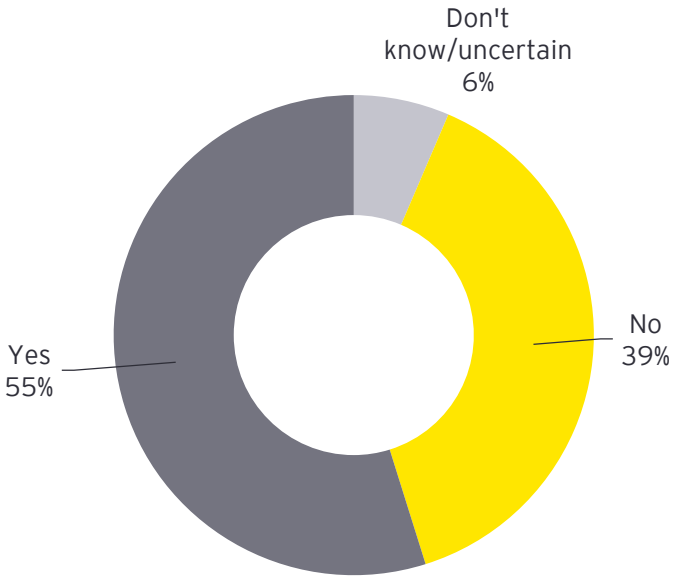
Q47. [If Yes] Are intercompany affiliates included in the golden-source third-party inventory or maintained separately?



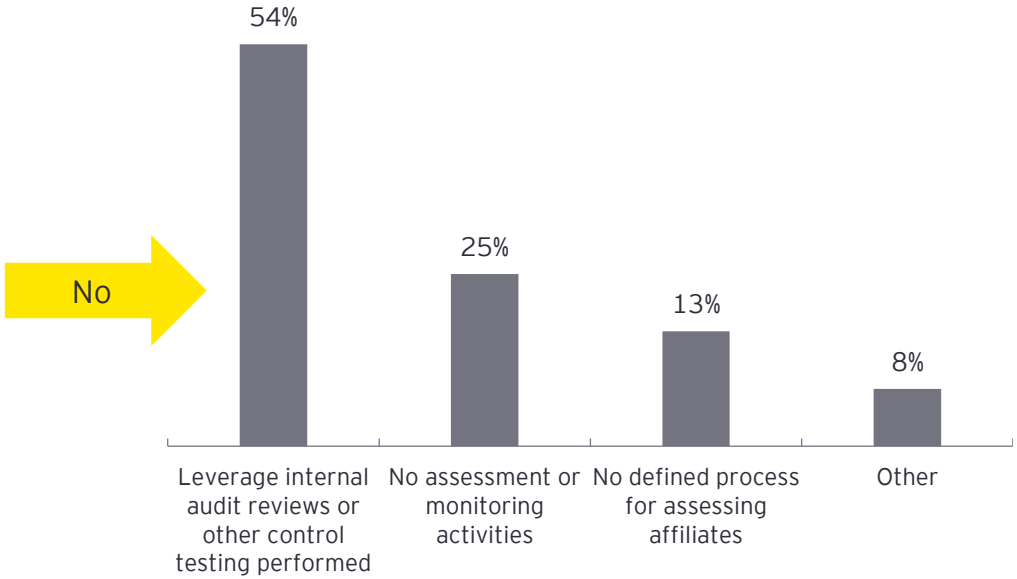
For those financial services organizations surveyed that have intercompany affiliates that are in-scope for their TPRM programs, 55% say that the process is the same for assessing them. For those organizations that have a different process, most are leveraging internal audit reviews or other control testing, suggesting that there are ways to rightsize affiliate management without additional assessment efforts.

Intercompany affiliates assessment process

Q48. Is your process for assessing internal affiliates the same as your third-party risk management process?



Q49. [If No] How is the process different for intercompany affiliates?

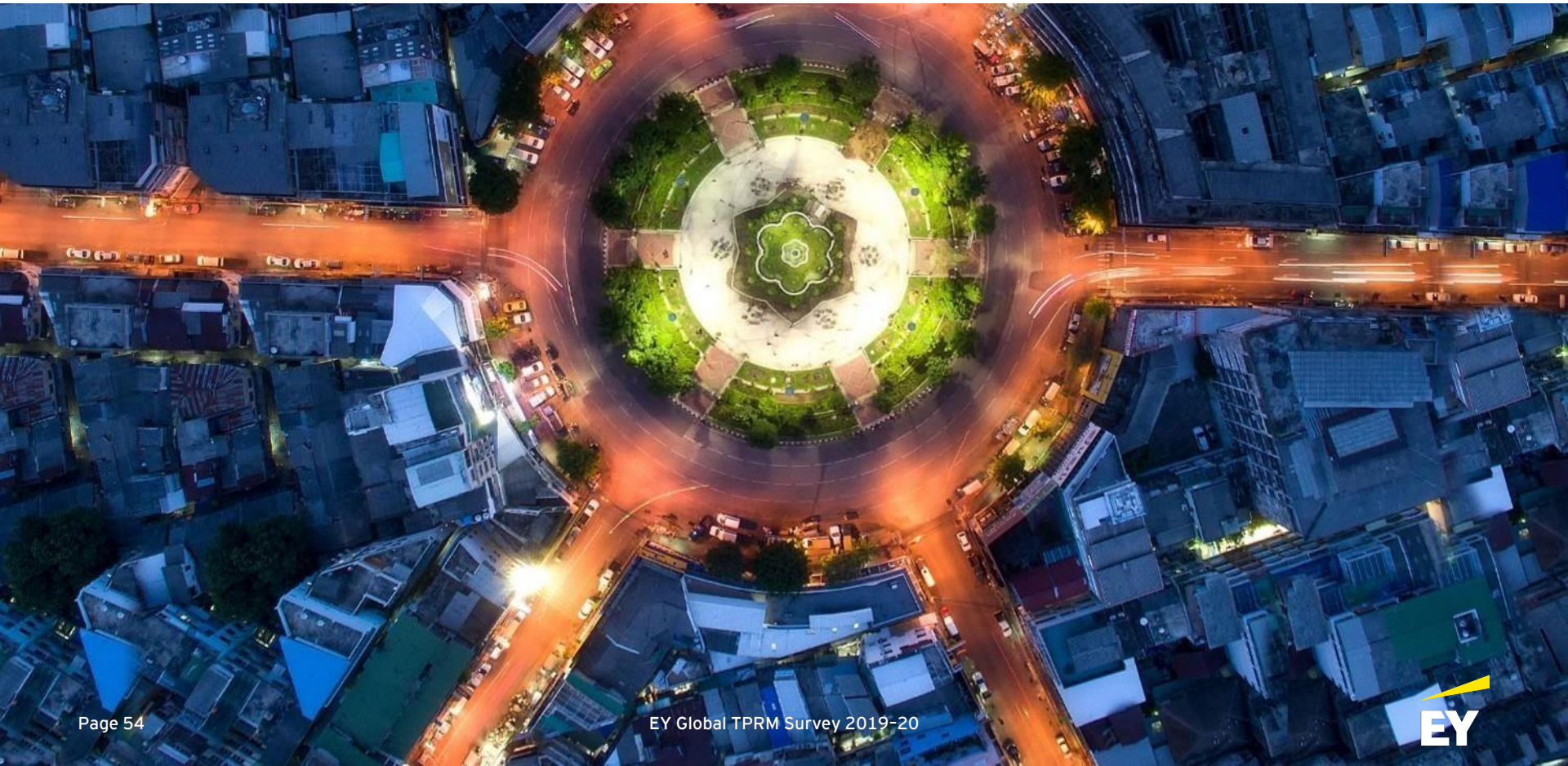


Affiliate monitoring requirements seem to vary greatly, without consensus on even the basic activities like service-level monitoring for financial services organizations.

Intercompany monitoring requirements

Q50. Which of the following ongoing monitoring requirements apply to intercompany affiliates providing goods/services to your organization?

Innovation

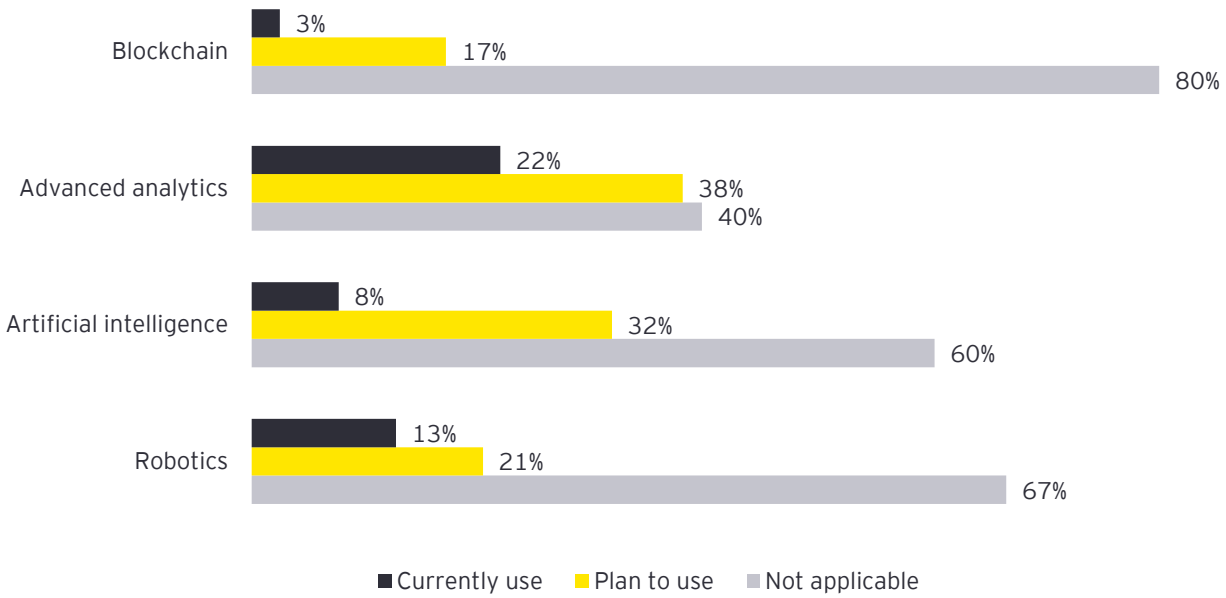


Just one in five financial services organizations surveyed are using advanced analytics, and even fewer are using AI, robotics or blockchain. However, organizations recognize the benefits that such technology can provide, as 38% of organizations plan to use advanced analytics and 32% plan to use artificial intelligence in the next two to three years.

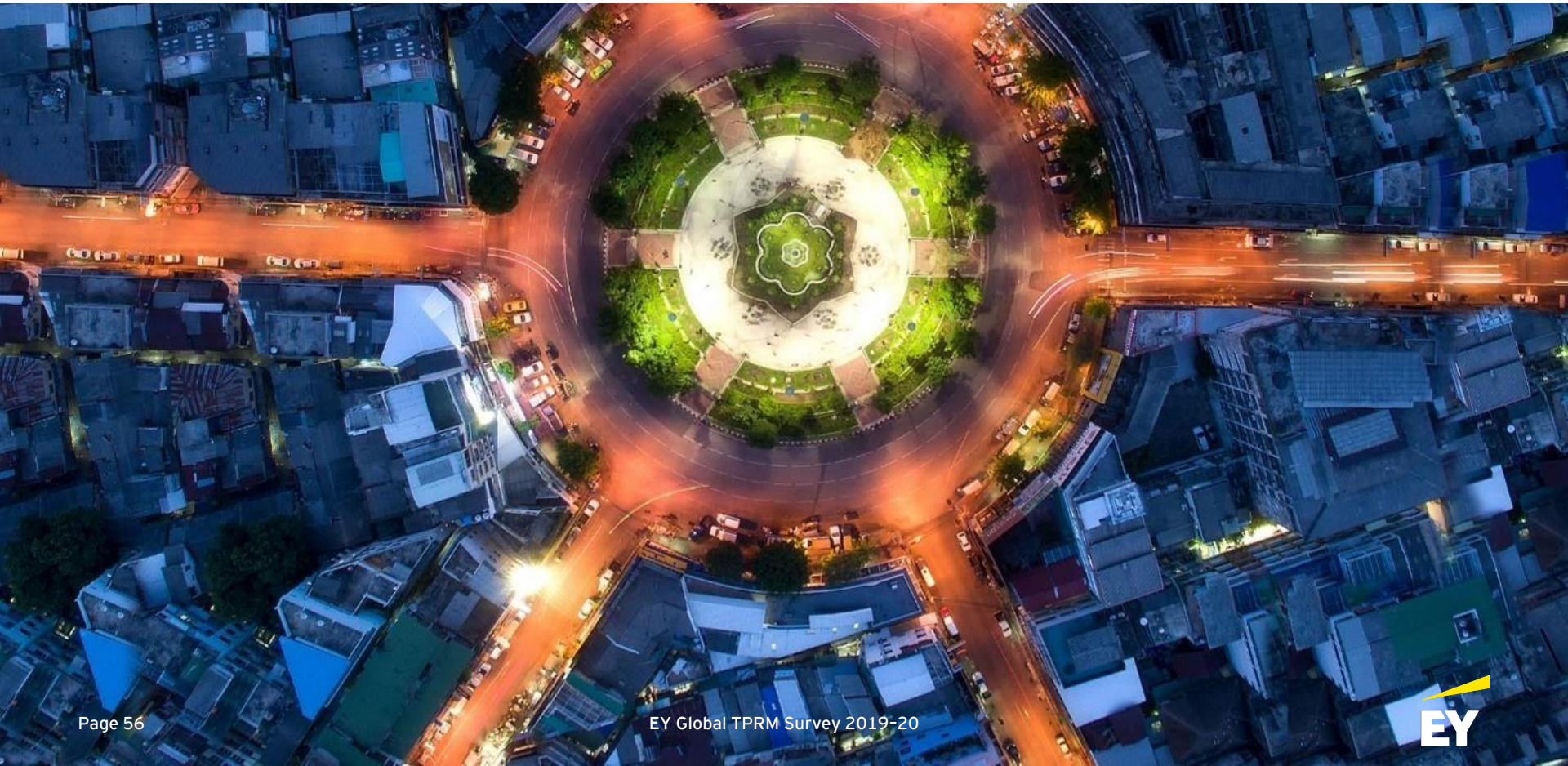
Emerging technologies for TPRM

Q51. 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?



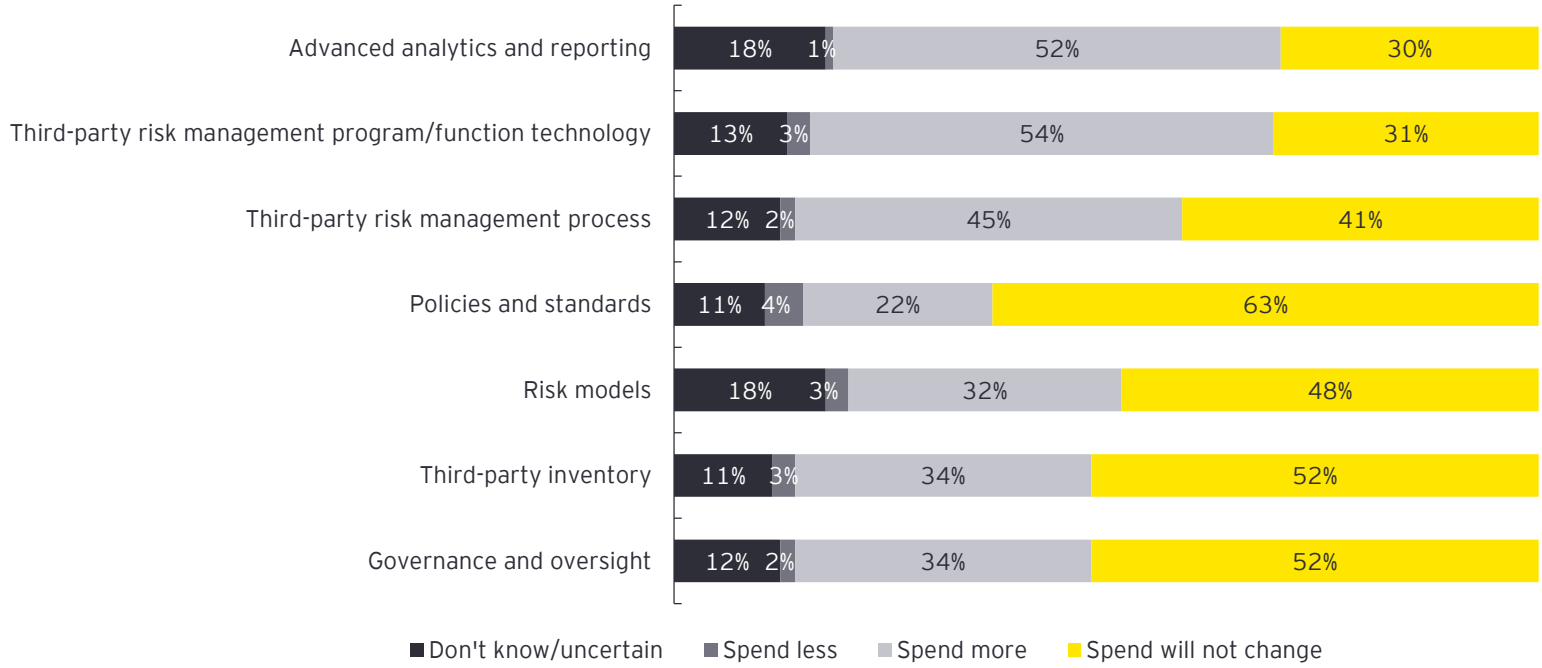
Areas of investment



In order to better leverage the technology they have and stay ahead of the curve when it comes to emerging technologies, over half of financial services organizations surveyed plan to increase their spending on technology supporting their TPRM programs and advanced analytics. Advanced analytics is the most common emerging technology currently used (Q51), and 52% of organizations plan to spend more in the future. Eighty-six percent of the organizations will maintain spend or increase spend for third-party risk management processes.

Time investment in activities

Q52. Compared with the current year, does your organization plan to spend more, less or the same amount for the following activities?



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.

002185-20Gbl
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 and Performance Improvement Leader
amy.brachio@ey.com
Tel: +1 612 371 8537

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

Americas

Matthew Moog
EY Global Financial Services TPRM Leader
matthew.moog@ey.com
+1 201 551 5030

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

Asia-Pacific

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

Oceania

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

Europe, Middle East, India and Africa (EMEIA)

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